

**DEVELOPING AND ASSESSING A CYBER-RESILIENCE FRAMEWORK FOR  
KENYAN BANKS.**

Maricus Otieno Mayunga

A Project Research Submitted in Partial Fulfilment of the Requirements for the Award of the  
Degree of Master of Science in Applied Information Technology in the Department of  
Computer and Information Technology and the School of Science and Technology of Africa  
Nazarene University.

June 2019.

## DECLARATION

I declare that this document and the research it describes are my original work and that they have not been presented in any other university for academic work.

Maricus Otieno Mayunga

Reg. No. 17m03dmit006

\_\_\_\_\_  
Signed

16/08/2019  
Date

This research was conducted under my supervision and is submitted with my approval as a university supervisor.

Kendi Muchungi, PhD

  
\_\_\_\_\_  
Signed

16/08/2019  
Date

Emily Otieno Roche, PhD

\_\_\_\_\_  
Signed

16/08/2019  
Date

Africa Nazarene University

Nairobi, Kenya

## **DEDICATION**

Almighty God – for the sustenance and good health.

To my family: For the support and the tolerance borne during my many hours of absence while conducting this research.

To my only daughter Jill, for willingly taking the role of a data entry operator, and for excellent editorial work on this document.

The late Dr. Geoffrey William Griffin has a special place in my heart. He gave me a place to stand.

## Table of Contents

DECLARATION .....	i
DEDICATION .....	ii
ABSTRACT.....	vii
ACKNOWLEDGEMENTS .....	viii
DEFINITION OF TERMS .....	ix
ABBREVIATIONS/ACRONYMS.....	xi
LIST OF FIGURES .....	xiii
LIST OF TABLES .....	xiv
CHAPTER ONE - INTRODUCTION.....	1
1.1    Introduction.....	1
1.2    Background of the Study .....	1
1.3    Research problem.....	3
1.4    Purpose of the Research Study .....	4
1.5    Objectives of the Study .....	4
1.5.1    Main Objective.....	4
1.5.2    Specific Objectives .....	4
1.6    Research Questions .....	5
1.7    Hypothesis of the Study .....	5
1.8    Significance of the Research Study .....	6
1.8.1    Why is cyber-resilience important for banks? .....	6
1.9    Scope of the Study .....	7
1.10    Delimitation of the Study.....	7
1.11    Limitations of the Study.....	7
1.12    Assumptions.....	8
1.12.1    Concepts of Key Cyber-resilience domain .....	8
1.13    Theoretical Framework.....	9

1.14	Conceptual Framework.....	15
1.14.1	Conceptual Framework Diagram.....	16
1.14.2	Conceptual Framework and hypotheses .....	17
CHAPTER TWO – LITERATURE REVIEW .....		18
2.1	Introduction.....	18
2.2	Theoretical Review of Literature .....	18
2.3	Empirical Review of Literature .....	19
2.3.1	Existing approaches to assessing Cyber-resilience.....	20
2.3.2	Constructs for measuring cyber-resilience.....	22
2.4	Selection of metrics for measuring Cyber-resilience in Banks.....	22
2.5	Research Gap .....	26
2.6	Summary of literature review .....	27
CHAPTER THREE – RESEARCH DESIGN AND METHODOLOGY .....		28
3.1	Introduction.....	28
3.2	Research Design.....	28
3.2.1	Research Plan.....	29
3.2.3	Framework and Research Instruments.....	30
3.3	Research Site.....	30
3.4	Target Population.....	30
3.5	Determination of Research Sample Size.....	31
3.5.1	Sampling Procedure .....	31
3.5.2	Study Sample Size .....	31
3.5.3	Sample Selection.....	32
3.6	Target Respondents.....	33
3.7	Sampling Design.....	33
3.8	Variables and Constructs .....	34
3.8.1.	Measuring and grading constructs .....	34
3.8.2.	Demographic variables .....	36
3.9	Data Collection measures .....	36

3.9.1	Question types.....	37
3.9.2	Distributing the instrument .....	37
3.9.3	Matters arising from the Pilot Study.....	37
3.9.4	Instrument Validity .....	38
3.9.5	Instrument Reliability .....	38
3.10	Ethical Considerations .....	39
3.11	Data Analysis Design.....	39
3.12	Data Analysis methods and tools.....	39
3.12.1	Analysis tools.....	39
3.12.2	Measures of Central Tendency .....	40
3.12.3	Measures of association or relationship measures.....	40
3.12.4	Pearson’s Correlation Coefficient (r).....	40
3.12.5	One-way Analysis of variance (ANOVA).....	40
3.12.6	Using one-way ANOVA to test for Hypothesis .....	41
CHAPTER FOUR – RESULTS AND ANALYSIS .....		42
4.1	Introduction.....	42
4.2	Response Rate.....	42
4.3.1	Response Rate Validity.....	43
4.3.2	Confirmation of Instrument Reliability .....	44
4.3	Presentation of findings .....	45
4.3.1	Demographics and relevance of Respondents .....	45
4.3.2	Responses per variable for measuring cyber-resilience.....	51
4.3.3	Analysis by Objectives .....	52
4.3.4	Identify and defining variables for measuring cyber-resilience .....	52
4.3.5	Analysis by constructs .....	52
4.4	Test of Hypotheses Analysis of Variance.....	72
4.4.1	Test of Hypotheses per predictor variables.....	77
4.5	Overall Cyber-resilience score and posture .....	95
CHAPTER FIVE – DISCUSSION, CONCLUSION AND RECOMMENDATIONS .....		97

5.1	Introduction.....	97
5.2	Discussions .....	97
5.2.1.	What are the acceptable instruments and indicators necessary for assessing cyber-resilience of Kenyan banks? .....	97
5.2.2.	To what degrees of measure are Banks in Kenya cyber-resilient? .....	97
5.2.3.	How many banks in Kenya are prepared if and when a cyberattack takes place? .....	98
5.2.4.	Do banks hide vulnerabilities and losses? .....	98
5.2.5.	Discussions on Constructs for measuring cyber-resilience .....	99
5.3	Summary of main findings.....	101
5.4	Conclusion .....	101
5.5	Recommendations.....	103
5.6	Areas of Further Research .....	104
	REFERENCES .....	105
	APPENDICES .....	110
	Appendix B – Consolidated List of Variables .....	111
	Appendix C – List of variables grouped by Construct .....	125
	Appendix D -Descriptive Statistics for each Response question.....	133
	Appendix E – Map of Nairobi showing research locations. ....	141
	Appendix F – Research Permits.....	144
	Appendix G – Survey letters.....	147
	Appendix H - Activity Plan for the Research project .....	149

## ABSTRACT

Rampant cyber incidences in Kenya targeting banks call for mediations beyond existing cybersecurity principles. This quantitative study sought to collate multi-domain variables from previous works to develop a framework for measuring cyber-resilience in Kenyan banks known as the Cyber-resilience Framework for Banks (CRF4Banks). The framework consists of eight key cyber-resilience constructs and their constituent variables, identified from empirical research and literature. Cyber-resilience has not received the attention it requires in Kenyan banks. Often conflated and confused with cybersecurity, cyber-resilience has not received as much attention as cybersecurity principles. Many reports on financial institutions in Kenya focus mainly on organisational and financial stability, done as part of annual financial audit, and ignore the role played by cyber-resilience. Compounding this, are the fragmented and competing cybersecurity assessments from a multitude of cybersecurity providers that lack coherence. The financial sector in Kenya needs its own unified framework and common measurement indicators, built from best practices, and curated for cyber-resilience. The research, through CRF4Banks, roots for an integrated approach towards measuring cyber-resilience. Three factors motivate this: first, because banks share a cyberspace with everyone else who are facing unlimited and borderless vulnerabilities, second, because these vulnerabilities have interlinked causative factors such as financial performance, organisation structure, ICT infrastructure, human; and lastly, because there is a public perception driven by media that banks in Kenya have been hiding cyber-attacks, fearing reputation damage. Kenyan banks were used as the target population. The research used descriptive research approaches augmented by quantitative techniques to measure the variables. The framework was first validated by cybersecurity 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. One cyber-security accountable respondent was provided by each bank to participate in an online and self-administered questionnaire, delivered to the respondents through Survey Monkey. Survey questions were close-ended Likert-scale types. Data was processed and analysed further using SPSS and Excel. The expected outcomes were, first, a comprehensive cyber-resilience framework instrument, second, a cyber-resilience status report of all banks. The expected outcome from the study was threefold: first, a comprehensive cyber-resilience instrument with localized variables for banks, second, a framework for measuring cyber-resilience, and lastly, a survey report showing cyber-resilience status of Kenyan banks. The cyber-resilience report seeks to confirm or disapprove the main null hypothesis that most Kenyan banks are not cyber-resilient. Finally, the tool was deployed in a survey and the outcome of the survey showed strong performances in all the eight constructs of cyber-resilience, contrary to adverse media reports. Besides providing a tool for assessing cyber-resilience, the research helped to foster cyber-resilience principles among banks. It also provides new dimensions for banks, offering insights into areas that remain unexploited such as cyber-crime risk transfer. Besides, the research also identified some areas of improvement such as the use of advance technologies, development of cyber law frameworks and the need for training law enforces on digital forensics.



## ACKNOWLEDGEMENTS

All the effort and time I invested in this project would have been in vain were it not for the gift of good health that the Almighty God bequeathed upon me during the period of compiling this research thesis. Not to forget the tolerance my family endured of my absence as I raced against time to complete this thesis.

Much appreciation goes to my thesis Supervisors, Dr. Kendi Muchungi and Dr. Emily Roche from whom I received valuable guidance, encouragement, contributions and criticism that helped shape the direction of the research. Behind the scene, there are many unforgettable individuals. From the School of Science and Technology, Dr. A. Gichamba, the Department of Computer and Information Technology (CIT) Chairman Mr. J. Obuhuma, Ms. C. Achieng' of the Department of Environment and Resource Management for their numerous contributions that have formed the backbone of this project thesis.

Much gratitude to Dr. Bonface Ileri Ngari (Multimedia University) and Mr. Aldrin Barasa (University of Nairobi) for accepting to be expert reviewers of the instrument developed in this research.

May the Lord reward you abundantly for all your efforts.

Heartfelt appreciations!

## DEFINITION OF TERMS

Business Continuity	A set of organisation processes formulated to identify and endure critical business processes remain functional when disasters occur (Whitman & Mattord, 2014).
Adaptive Capacity	The degree to which a system can modify its circumstances to move to a less vulnerable condition or back to the original state before the vulnerability (Luers et al, 2003; Dalziell and McManus, 2008).
Computer Emergency Response Team	A Computer Emergency Response Team (CERT) is an expert group that handles computer security incidents. Many countries have formulated local CERT teams, which have adopted the initials CSIRT (Computer Emergency Readiness Team and Computer Security Incident Response Team).
Cybersecurity	The protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.
Cybercrime	An act committed on the cyberspace, on or using computer, and in which such an act is explicitly defined as a crime within the context of the law jurisdiction. The computer is the object of the crime or is used as the tool for committing the crime (Technopedia.com).
Cyber-resilience	The ability of an organization to continue its existence or to remain more or less stable in the face of shock or deprivation of resources or from a physical threat
Cyberspace	The virtual reality or notional environment in which electronic communication (mostly Internet-based) occurs (Oxford English Dictionary, 2009 Edition).

- Disaster Recovery** Part of a wider plan consisting of processes aimed at preparing an organisation to recover from disaster if and when it happens (Whitman & Mattord, 2014).
- Penetration Testing** A process in which personnel perform an authorized/controlled simulated cyber-attack with the aim of evaluating existence of vulnerabilities (Whitman & Mattord, 2014).
- Vulnerability** Within the context of cyberspace, a vulnerability is a weakness in a system that allows a threat to compromise its security (Harris & Maymí, 2016, p.6).

## ABBREVIATIONS/ACRONYMS

ANOVA	Analysis of variance
ANU	Africa Nazarene University
BC	Business Continuity
BR	Business Resilience
CBK	Central Bank of Kenya
CERT	Computer Emergency Response Team of Carnegie Mellon University.
CERT-RMM	CERT Resilience Management Model
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
CRF4Banks	Cyber-Resilience Framework for Banks.
CRO	Chief Risk Officer
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security.
DTMB	Deposit-Taking Microfinance Bank
IBM	International Business Machines
ICT	Information and Communication Technology
ISO	International Standards Organisation
ISO/IEC	International Standards Organisation /International Electrotechnical Commission
IT	Information Technology
ITU	International Telecommunication Union.
KE-CIRT/CC	Kenya Computer Incident Response Team Coordination Centre
KES	Kenya Shilling
KICA	Kenya Information Communication Act
NACOSTI	National Commission for Science, Technology and Innovation.
NIST	National Institute of Standards and Technology

SACCO	Savings and Credit Cooperative Organisation.
SANS	SysAdmin, Audit, Network and Security
SASRA	SACCO Societies Regulatory Authority
SD	Standard Deviation
SME	Subject-Matter Expert
SPSS	Statistical Package for Social Scientists.
URL	Universal Resource Locator

## LIST OF FIGURES

	<b>Page</b>
Figure 1-1. Relationship between Resilience, Vulnerability and Adaptive capacity	9
Figure 1-2. Resilience of system functions over time .....	10
Figure 1-3. Notional resilience profile: system's critical functionality over time ...	10
Figure 1-4. Fig 1-4: Seven-point cyber-resilience framework by Ponemon .....	12
Figure 1-5. Figure 1-5: Schematic diagram of adopted frameworks .....	14
Figure 1-5. Conceptual Framework Diagram .....	16
Figure 1-6. Relationship between Conceptual Framework Diagram and Hypotheses	17
Figure 4-1. Response rate .....	42
Figure 4-2. Break-down of target population by peer group size .....	44
Figure 4-3. Demographic of respondents by Role focus .....	45
Figure 4-4. Demographic of respondents by Position level. ....	46
Figure 4-5. Demographic of respondents by reporting channel. ....	47
Figure 4-6. Staff head count of respondent banks .....	47
Figure 4-7. Full head-count of cyber security team at the bank. ....	49
Figure 4-8. Full-time equivalent (FTE) headcount required. ....	49
Figure 4-9a. Scatter and regression graph for correlation between (a) Agility and Governance, leadership and Compliance, and .....	56
Figure 4-9b. Scatter and regression graph for correlation between Agility and Preparedness .....	56
Figure 4-10. Respondent banks that conduct cybersecurity awareness to staff. ....	62
Figure 4-11. Handling of cyber-incidents by law enforcers .....	64

## LIST OF TABLES

	<b>Page</b>
Table 1-1 Comparison of old and new factors for measuring cyber-resilience.	13
Table 2-1 Constructs for measuring cyber-resilience.....	22
Table 3-1 Sample Size Distribution by peer size .....	33
Table 3-2 Ranking and grading scheme for cyber-resilience.....	35
Table 4-1 Response statistics .....	43
Table 4-2a Comparing reliability statistics for the pilot study and main research instruments .....	45
Table 4-2b Demographic of respondents by Activities done as part of role	46
Table 4-3 Descriptive Statistics for comparing full-time head count in IT department vs desired head count for achieving cyber-resilience .....	48
Table 4-4 Correlation of Current IT head count vs required capacity to cyber- resilience .....	50
Table 4-5 Perception to cyber-resilience constructs .....	53
Table 4-6 Correlation matrix between Cyber-resilience variables .....	55
Table 4-7 In the past 12 months, how has the time to detect, contain and respond to a cyber-crime incident changed? .....	58
Table 4-8 Existence of cyber-security incident response plan (CSIRP .....	59
Table 4-9 If you have a Disaster Recovery (DR) plan, how often is it reviewed and tested? .....	60
Table 4-10 Rating for cyber-resiliency with regards to your Service level recoverability .....	60
Table 4-11 Rating for cyber-resiliency with regards to your Service level objective .....	61
Table 4-12 Participation in initiatives for information sharing .....	64
Table 4-13 Reasons why bank would share information about its data breach	65
Table 4-14 What drives the bank to invest in information security .....	67
Table 4-15 Pearson correlation- Staff head counts. ....	68
Table 4-16 IT security headcount vs target .....	69
Table 4-17 Assessing factors that influence Agility .....	70

Table 4-18	What best describes the maturity level of the bank's cybersecurity program or activities? .....	72
Table 4-19	Summary of Status of Hypothesis testing .....	74
Table 4-20	Model Summary – all variables together .....	75
Table 4-21	ANOVA– all variables together .....	76
Table 4-22	Coefficients– all variables together .....	76
Table 4-23	Model Summary for Agility .....	77
Table 4-24	Analysis of variance (ANOVA) for Agility perceptions on cyber-resilience .....	78
Table 4-25	Model Summary for Preparedness .....	78
Table 4-26	Coefficients for Preparedness perceptions on cyber-resilience.....	79
Table 4-27	Analysis of variance (ANOVA) for Preparedness perceptions on cyber-resilience .....	79
Table 4-28	Model Summary for Strong Security Posture .....	80
Table 4-29	Analysis of variance (ANOVA) for Strong Security posture perceptions on cyber-resilience .....	81
Table 4-30	Coefficients for Strong Security posture perceptions on cyber-resilience... ..	81
Table 4-31	Model Summary for Redundancy Planning.....	82
Table 4-32	Analysis of variance (ANOVA) for Redundancy Planning effects on cyber-resilience .....	83
Table 4-33	Coefficients for Redundancy Planning effects on cyber-resilience..	83
Table 4-34	Model Summary for Knowledgeable or Expert Staff .....	84
Table 4-35	Analysis of variance (ANOVA) for Knowledgeable or Expert Staff effects on cyber-resilience .....	85
Table 4-36	Coefficients for Knowledgeable or Expert Staff on cyber-resilience	85
Table 4-37	Model Summary for Ample resources .....	86
Table 4-38	Analysis of variance (ANOVA) for Ample resources effects on cyber-resilience .....	87
Table 4-39	Coefficients for Ample resources on cyber-resilience .....	87
Table 4-40	Model Summary for Governance, Leadership & Compliance .....	88
Table 4-41	Analysis of variance (ANOVA) for effects of Governance, Leadership and Compliance on cyber-resilience .....	89
Table 4-43	Model Summary for Asset Classification & Risk Profiling .....	90



Table 4-44	Analysis of variance (ANOVA) for effects of Asset Classification & Risk Profiling on cyber-resilience .....	90
Table 4-46	Cyber-resilience weighted mean and strength grade score .....	91
Table 4-47	Grading of Respondent cyber-strength per construct .....	93
Table 4-48	Weighted mean of Cyber-strength by constructs .....	93
Table 4-49	Participants grouped by cyber-resilience strength and construct .....	95

# CHAPTER ONE - INTRODUCTION

## 1.1 Introduction

This chapter describes and sets the context for the research project. It provides background to the research topic, defines the problem statement, purpose and objectives motivating the research, and also sets the research questions and hypothesis. It delves into detail to describe the various existing cyber-resilience frameworks, reviews and amalgamates features of key frameworks and standards into a conceptual framework. Anchoring on Ponemon Institute's Cyber-resilience framework, the section collates features from other standard frameworks and research literature on cyber-resilience. The outcome is a hybrid framework, hypothesized and conceptualised in section 1.16. This new framework is elaborated further in Chapter two.

## 1.2 Background of the Study

The term "resilience" (Latin word for *resilio* meaning "jump back") has been used widely in general applications and discourses. Comfort, Boin and Demchak (2010) define resilience in general context as the ability of an organization to continue its existence or to remain more or less stable in the face of shock or deprivation of resources or from a physical threat. When conflated with cyberspace, resilience transforms into cyber-resilience.

Rampant cyber security incidents have necessitated research into and discourses on cyber-resilience (Obura, 2017). Many corporate organisations and governments have realized that despite huge investments in cybersecurity defenses, cybercrime incidents are still increasing in frequency and in sophistication. Nowhere has this concern reached a critical level as it in Kenya, specifically among banks. If recent high profile cyber incidences in which banks lost thousands of US dollars (BBC, 2016; Ombati, 2017; Olingo, 2018; Sunday, 2019; Muthoni, Karanja & Sunday, 2019) are anything to go by, banks need to place cyber-resilience as a top priority. Kenya lost over US\$ 22.56 million (approximately KES 2.3 billion) to cyber-crime in 2013 (Otieno, 2014), with this growing by 40% in 2015 (Symantec, 2016) vectored mainly by malware. This translated to a loss of KES 17.1 billion (Cisco, 2017). In 2016, the Kenya Revenue Authority alone had a loss of KES 4 billion (approximately US\$ 39 million) from hackers (Kakah, 2016). This grew further by 22% in 2017 (Serianu, 2017). Serianu

(2017) avers that 72% of the institutions affected by cybercrime did not report to the authorities.

These losses and incidences came in at a time when heightened multi-sectoral stakeholder action was being instigated. 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 (suspended by court in 2019); CBK has also enforced cyber-security and incident monitoring vide a regulatory note (CBK, 2017). Outside Kenya, the Asia Bankers Association declared that cyber-resilience is the future of cybersecurity (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 defences launched the Cyber Resilience for Development (Cyber4Dev) encompassing four countries in Asia and Africa (EU, 2017, 2019). Other governments have also been at the forefront of formulating policies and partnerships to secure the cyberspace (HM Government, 2016 & Crown, 2009). International Telecommunications Union (ITU) has been actively pushing governments to form National Computer Incident Response Team Coordination Centre or National CIRT/CC (ITU, 2017) to provide local cyber-incident response units. The National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) was formed in 2015 as a result of this initiative.

All these interventions need to be consolidated into the broader realm of cyber-resilience and localised. In Kenyan banks, cyber-resilience discussions are in infancy stages, while adoption is mainly driven by the regulatory arm of CBK. Banks need to transform beyond traditional cybersecurity approaches, most which presupposes cyber-defenses from a known-risk perspective. IBM (2011) highlights this transformation, contending that in the mid-1990s, disaster recovery (DR) was the most popular IT resilience practice but it gave way to business continuity (BC); BC recently transformed to business resilience (BR) comprising of such elements as availability, recovery, security and compliance techniques. Thus, many organisations now content that no amount of cyber-security will prevent cyber-attacks. That inevitability of cyber incidents is pushing organisations to focus on how to reduce their impact while remaining in operation. This is the essence of deepening cyber-resilience.

This paper, therefore, purposes to incorporate the foregoing strategies within the context of best practices, empirical researches, standards and frameworks, such International Standards Organisation (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), and Computer Emergency Response Team-Resilience Management Model (CERT-RMM) to formulate a framework code-named Cyber-resilience Framework for Banks (CRF4Banks) specifically suited for measuring cyber-resilience of banks in Kenya. Such a framework, according to Cooper and Schindler (2014), will help banks to characterise the multitude of cyber-resilience indicators into a system or methodology. Finally, using the framework's instrument, conduct a survey of cyber-resilience of Kenyan banks – and provide the cyber-resilience status of the banks in Kenya.

### **1.3 Research problem**

In Kenya, there is no standard methodology or framework for measuring cyber-resilience of banks. Traditionally, banks follow prudential guidelines and best practice in their operations; cyber-resilience never features as a reporting line in the financial reports. According to the CBK (2017a), banks in Kenya were “resilient during a perfect storm” having weathered political turbulence in 2017 to post above-average capital adequacy of 18.8% and liquidity ratio of 43.7%, the two main benchmarks that it used for measuring resilience of banks in Kenya. This clearly indicates that the CBK did not place cyber-resilience at the core of its reporting. A separate guidance note on cybersecurity reporting was formulated in 2017 (CBK, 2017b) that defines certain cybersecurity principles and reporting. Comprehensive cyber-resilience reporting is an essential ingredient for deepening cyber-resilience principles. This research therefore, purposes to develop a framework for measuring cyber-resilience of Kenyan banks. This is hoped to deepen cyber-resilience best practice.

Secondly, although much research exists in cybersecurity assessments, what the Kenyan environment lacks is a unified approach to measuring cyber-resilience. Existing methods of measuring cyber-resilience have been fragmented and punctuated with competing interests. Most cyber reports are produced by international cybersecurity firms. These reports lack the local depth and breadth. Confirming this assertion, Kott and Linkov (2019, p.10) allude to the current lack of universally adopted resilience

metrics and the inability to formalize value systems for the existing methods, as major drawbacks of wide adoption of metric-based methodologies. There are different organisations already providing annual cyber-security status reports, each with varying measurement variables. This research therefore, purposes to solve the following problems:

- a) Lack of a localised standard framework for measuring cyber-resiliency of banks in Kenya is a hindrance to understanding banks' level of resilience.
- b) The fragmented cyber-resilient strategies, measurement indicators and reporting by banks calls for harmonization into a unified framework for assessing cyber-resilience of Kenyan banks.
- c) Banks have concentrated of cyber-security. There is need to embrace cyber-resilience. This is currently lacking because cyber-resilience is still a developing domain and assessment methods have not stabilized into concrete frameworks.

#### **1.4 Purpose of the Research Study**

The purpose of this research is threefold. First, to develop a localized framework for assessing cyber-resilience in Kenyan banks. Second, to validate and assess the framework through a survey that will assess cyber-resilience strength of the banks.

#### **1.5 Objectives of the Study**

##### **1.5.1 Main Objective**

The main objective is to collate best-practise measurement indicators and develop a localized framework for measuring cyber-resilience in Kenyan banks, and then use the framework to assess the cyber-resilience strength of the banks.

##### **1.5.2 Specific Objectives**

The following specific objectives were formulated to achieve the aforementioned main objective:

- i) To identify relevant measurement variables, indicators and strategies necessary for enhanced cyber-resilience of Kenyan banks.
- ii) To development a framework for measuring cyber-resilience in Kenyan Banks.

- iii) To assess the framework developed by measuring cyber-resilience posture of banks in Kenya.

### 1.6 Research Questions

This research seeks to answer the following questions:

RQ1: Are banks in Kenya cyber-resilient?

RQ2: What variables are necessary for assessing cyber-resilience of Kenyan banks?

RQ3: What are the indicators for measuring cyber-resilience of Kenyan banks?

### 1.7 Hypothesis of the Study

A hypothesis is a proposition (or set of it) defined to explain occurrence of a specified phenomenon, either inserted as a provisional conjecture either to guide a research or be accepted as plausible in light of derived facts (Kothari, 2004, p184). Thus, it measures the relationship between variables being studied and their prevalence in the phenomenon. This research has used null hypothesis. The following hypotheses have been floated and broadly identified for carrying out the study.

---

#### Null Hypotheses

---

***H<sub>0</sub><sub>1</sub>***: Majority of banks in Kenya are not cyber-resilient

***H<sub>0</sub><sub>2</sub>***: Agility factors do not have an effect on cyber-resilience enhancement perceptions in banks.

***H<sub>0</sub><sub>3</sub>***: Preparedness factors do not have an effect on cyber-resilience enhancement perceptions in banks.

***H<sub>0</sub><sub>4</sub>***: Strong security posture has no bearing on cyber-resilience enhancement perceptions in banks.

***H<sub>0</sub><sub>5</sub>***: Redundancy planning has no effect on cyber-resilience enhancement perceptions in banks.

***H<sub>0</sub><sub>6</sub>***: Knowledgeable and expert staff have no effect on cyber-resilience enhancement perceptions in banks.

**H0<sub>7</sub>:** Ample resources do not have effect on cyber-resilience enhancement perceptions in banks.

**H0<sub>8</sub>:** Governance, leadership and compliance factors have no effect on cyber-resilience enhancement perceptions in banks.

**H0<sub>9</sub>:** Classification and risk profiling of assets have no bearing on cyber-resilience enhancement perceptions in banks.

---

## **1.8 Significance of the Research Study**

The rapid digitisation of the Kenyan economy has brought with it many challenges, when looked at from the perspective of the cutting-edge financial technologies such as M-pesa. Gagliardone and Sambuli (2015) laments that this rapid digitisation and the dependency it propagates on the economy calls for measures to protect the digital economy against disruptive cyber threats. With the inevitability of cyber-attacks, banks need to look beyond the traditionally focus on cybersecurity without according due attention to broader resilience when conducting business in cyberspace. The research will contribute to the adoption of a localized cyber-resilience measurement framework for banks. The proposed research will also contribute to scholarly knowledge in cybersecurity best-practice. Additionally, from a cyber-resilience standpoint, the results of the research survey will provide a confidence rating of banks on their cybersecurity posture. The result of the study will not only stir action but also propagate cyber-resilience best practice beyond the financial sector of Kenya and the region. This is because organisations share a common cyberspace ecosystem. That means that successful cyber-resilience strategies will find their way to other institutions including government.

### **1.8.1 Why is cyber-resilience important for banks?**

Folke (2006, p.259) sums up the great benefit of being resilience: Not only does it breed persistence and robustness in the face of a disruption, it also brings opportunities that disruptions open up in terms of recombination of evolved infrastructures and processes, renewal of the system and the emergence of new trajectories.

The global cyberspace monoculture has created a potent attack targets that can be exploited by criminals, what with the rapid digitisation of every aspect of human life. Cyber attacks are therefore lurking and attacks are inevitable no matter how much in-depth cyber security principles are implemented. What will matter is how fast a bank can recover from such vulnerabilities. This is the principle behind cyber-resilience.

### **1.9 Scope of the Study**

Due to the ever changing vulnerability landscape in the cyberspace, the research was restricted to a period of one month between February and April, 2019. This is to ensure that all the references to the outcome are referenced to a point time. The validity of the outcome of the research and its instrument will however remain applicable for as long as the technological strategies in it have not become obsolete.

### **1.10 Delimitation of the Study**

The research focused on banks and mortgage institutions in Kenya excluding Cooperative Societies and Microfinance institutions. The Kenya Bankers Association lists 47 operational banks in Kenya as members (Kenya Bankers Association, 2019). The membership is a mix of commercial banks, mortgage bank and Deposit-Taking Microfinance Banks (DTMB) – all under the ambit of the CBK.

Respondents from the participating institutions were also restricted to subject-matter experts (SMEs) at the level of managers in charge of ICT and/or cybersecurity, and who report to the top-most executive. The study did not include other staff in the bank such as Operations, Finance, Executives and subordinate staff. The success of the research and the integrity of the data collected depended largely on the knowledge and expertise of the respondents in the domain of cybersecurity.

### **1.11 Limitations of the Study**

The dynamics of cyber-resilience in an organization, like resilience in general is multifold and traverses different aspects in an organization viz: human, organizational, financial, environmental, legal and so on (Comfort, et al., 2010). The dynamics of a framework for measuring cyber-resilience delves into technological factors which



become obsolete very fast. Therefore, there is possibility that some of the cyber-resilience measurement methods may not be applicable soon.

Kott and Linkov (2019, p.10) also adds that cyber-resilience consists of a big list of evaluation metrics. Designing these into an acceptable instrument is one thing but utilizing the measures is another challenge owing to their data-intensive requirements.

Furthermore, there is possibility of non-response bias, caused by a difficulty of reaching targeted respondents. Also, due to fear of data leakage and reputation damage, some bank respondents were conservative in participating. A high rate of no-response can skew the research results.

Finally, the integrity of the results can be influenced by other pressures such as media reports, legal restrictions and fear of data leakage.

## **1.12 Assumptions**

This research was designed and implemented based on the following assumptions:

1. That the outcome of the research would depend on the truthfulness and honesty of the respondents.
2. That there would a high response rate from participating banks to lend credence to the high credibility that the research seeks.

### **1.12.1 Concepts of Key Cyber-resilience domain**

#### **Resilience vs Cyber-resilience**

Cyber-resilience conflates general resilience with cyberspace to contextualize it with cyberspace. According to Linkov and Kott (2019), cyber-resilience is the ability of a system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyberattacks. Achieving resilience or cyber-resilience is viewed in relation to vulnerability and adaptive capacity (Comfort, et al., 2010). From the diagram below (Figure 1-1), making a system less vulnerable and increasing its adaptive capacity increases its resilience. In this case, the system's adaptive capacity are tilting the equilibrium upward to counter the downward pressures being exerted by vulnerabilities. In so doing, resilience is maintained or improved.

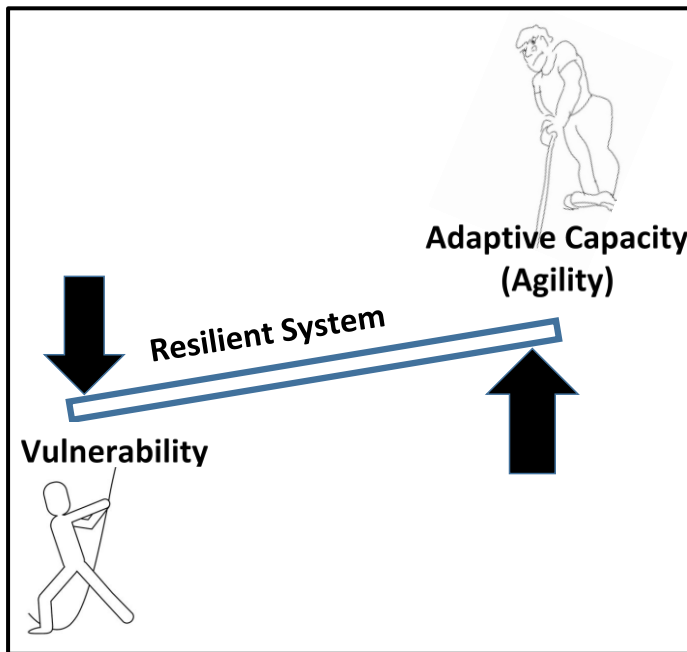


Figure 1-1: Relationship between Resilience, Vulnerability and Adaptive capacity (SOURCE: Comfort, et al., 2010, p.23)

### 1.13 Theoretical Framework

Cyber-resilience is a relatively new area, unlike general resilience, and it is still growing. Modelling or constructing cyber-resilience strategies have been known to take the approach of game theory. This is because the attack surface is very wide and the strategies are non-probabilistic. For every adversarial action, a countering defense strategy needs to be defined. Such strategies, like a hide-and-seek game, follow what Attiah, Chatterjee and Zou (2018) describe as Mixed Strategy Nash Equilibrium (MSNE), where each player in the game always has the incentive to deviate to another (randomize) strategy in order to wad the other off. Clearly, defenses implementing cyber-resilience must not utilise static analytical strategies. They must be as adaptive as the threats can be. By using the predictive power of game theory, combined with cyber deception, cyber agility, it is possible to form a robust cyber-resilience framework for proactive cyber defense. The ultimate goal of the proactive defense mechanisms is to ensure that system performance recovers from the shock caused by the cyber incidents. According to NIST, a cyber-resilient system ought to be built on five tenets of Plan, Prepare, Absorb, Recover and Adapt.

Figure 1-2 illustrates this concept in an example of a cyber-resilient organisation that has implemented proactive defense mechanisms that help plan, prepare, absorb, recover and adapt to threats.

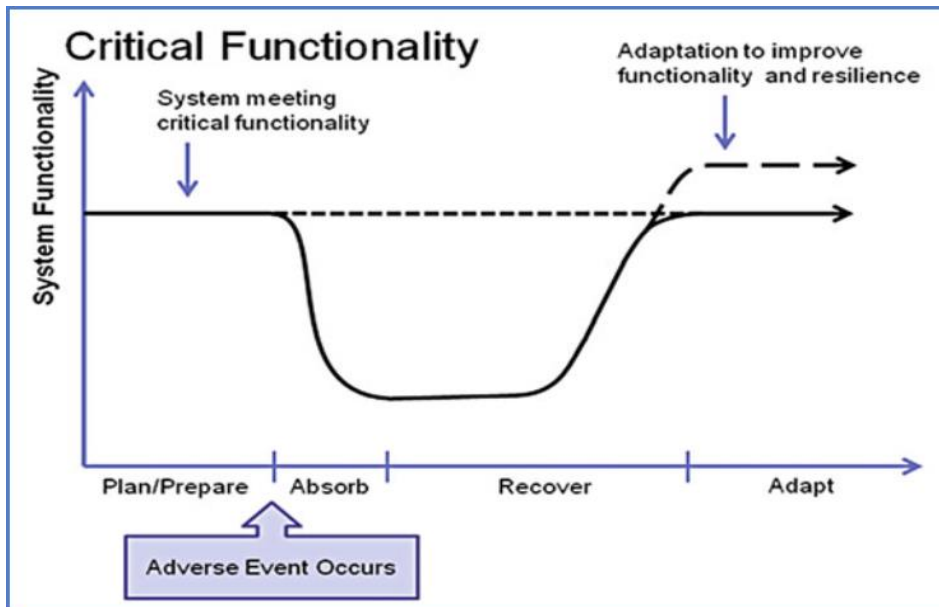


Fig 1-2: Resilience of system functions over time (SOURCE: Linkov & Kott, 2019, p.6)

Figure 1-3 plots a well-performing system suddenly hit by a cyber-attack degradation at time  $T_D$ , and the eventual self-recovery commencing at time  $T_R$ .

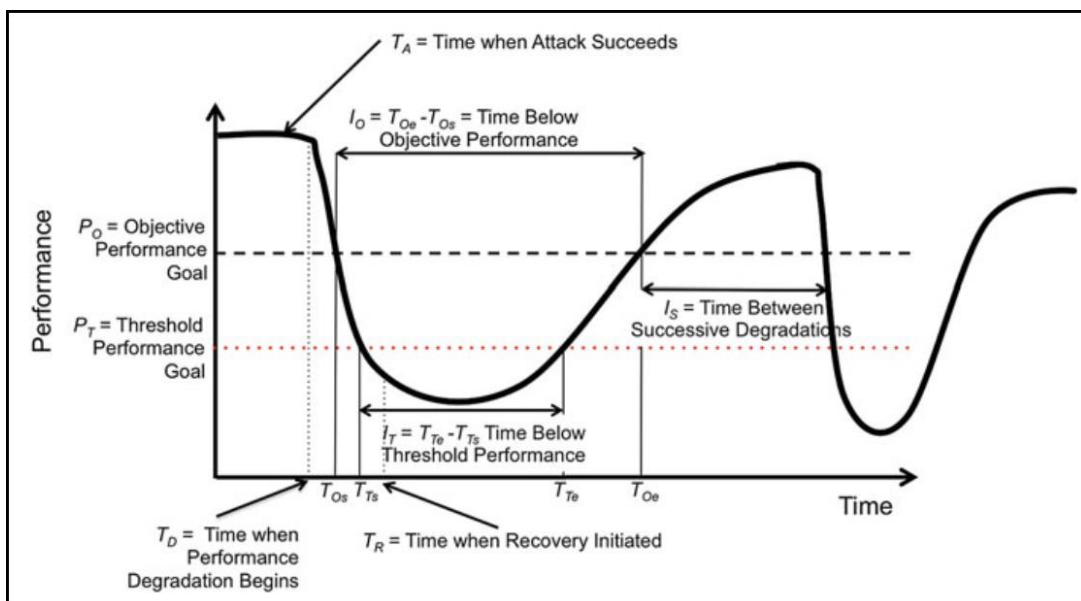


Fig 1-3: Notional resilience profile: system's critical functionality over time (SOURCE: Linkov & Kott, 2019, p.32)

The idea of modeling frameworks to address cyber-safety and cyber-resilience has been documented previously by Salim and Madnick (2016) and Antonucci (2017). Kott and Linkov (2019) also present two approaches that are popular in cyber-resilience literature. These are metric-based and model-based approaches. On the other hand,

NIST model contains twenty-one categories (Figure. 1.2c) for measuring cybersecurity, spread into five broad functions. These are governance of cybersecurity risk, control of access to assets and systems, awareness and training, detection and monitoring, and responsive actions. Shapiro and Keys (2019, p.71) cover these categories in a representation of functional areas with the main theme focusing on utilisation of organisation's business processes in order to guide its cybersecurity activities and internalisation of cybersecurity within the organisation's risk management processes. This framework was developed by Rutgers University for the Centre on Local Government Research Framework (Shapiro & Keys, 2019).

Caralli, et al. (2016) have also detailed a holistic CERT Resilience Management Model (CERT-RMM) covering a variety of resilience metrics. The twenty-seven metric categories overlap in many ways with NIST's twenty-one categories (Figure 1-5).

One of the key frameworks adopted by this research is that developed by Ponemon Institute for cyber-resilient organisation. Ponemon's cyber-resilience framework has been used in several surveys (Ponemon, 2019; Ponemon, 2018; Ponemon, 2017; Ponemon 2015). It bases its instrument on seven key factors for measuring cyber-resilience, namely: agility, strong security posture, knowledgeable and expert staff, leadership, planned redundancies, ample resources and preparedness (See Fig 1-4). The framework mirrors in many ways to NIST's framework, but misses certain key elements. It also borrows many principles from CERT-RMM. Apart from NIST, CERT-RMM and Ponemon, other frameworks whose idea have been borrowed to provide a local appeal include Serianu (2015), and regulatory policies from CBK (2017b).



Fig 1-4: Illustration of Seven-point cyber-resilience framework by Ponemon (Ponemon, 2015).

The challenge is to frame cyber-resilience as a characteristic of comprehensive cyber-security properties with cross-domain applications (Linkov & Kott, 2019). Figure 1-5 provides a schematic summary, of the frameworks, models and existing research frameworks that have been used to formulate this research framework. The diagram depicts the convergence of properties of existing frameworks and models into a new cyber-resilience framework.

The new framework modifies the seven-point Ponemon Institute framework into an 8-category framework, summarised in table 1-1 below:

**Table 1-1: Comparison of old and new factors for measuring cyber-resilience**

	<b>Current PONEMON framework</b>	<b>Changes</b>	<b>New framework</b>
1	Agility	Retained	Agility
2	Security Posture	Retained	Security Posture
3	Knowledgeable or expert staff	Retained	Knowledgeable or expert staff
4	Leadership	Amended	Leadership, +Governance and +Compliance
5	Planned redundancies	Retained	Planned redundancies
6	Ample resources	Retained	Ample resources
7	Preparedness	Retained	Preparedness
8		New	+ Asset classification and risk profiling

Table 1-1 summarises the main building blocks of the Ponemon Institute framework and the new framework. As shown on the table, most of what existed in the Ponemon Institute instrument has been incorporated into the new instrument. The new elements added have been sourced from other multiple frameworks such as NIST, CBK, Serianu and CERT-RMM. Figure 1-5 shows the complete list of the sources of the constructs used in building the new cyber-resilience framework.

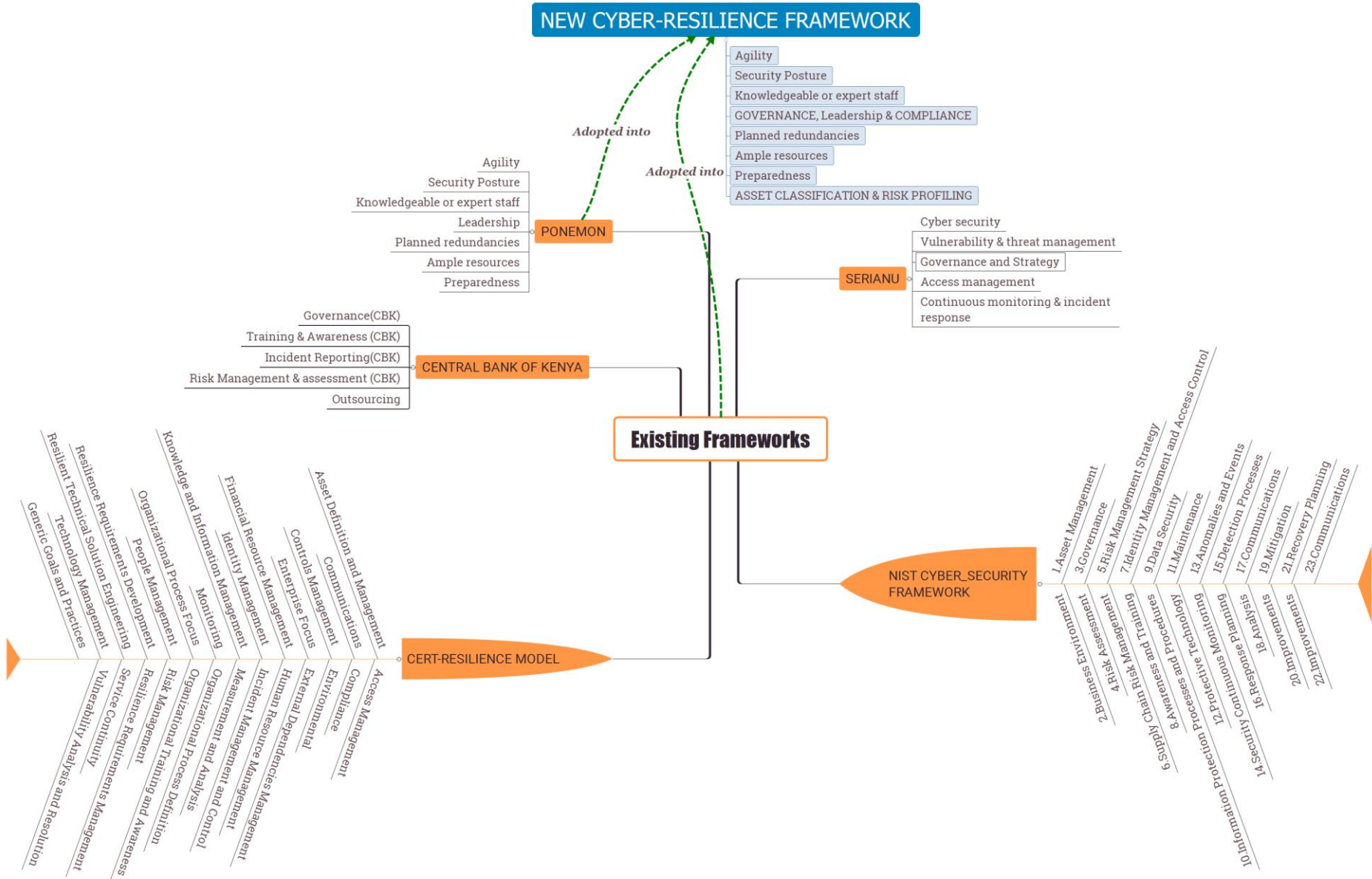


Figure 1-5: Schematic diagram of adopted frameworks

### **1.14 Conceptual Framework**

Based on cyber-resilience literature and theoretical review, and taking into consideration the research problem and objectives, a working conceptual framework was developed. The research has used the refined eight key constructs as key pillars for characterizing bank's cyber-resilience. These eight constructs were transformed into eight independent variables for measuring cyber-resilience strength. Hence, this paper proposes that the relationship between cyber-resilience strength and the independent variables can be studied empirically for the following dimensions: preparedness, agility, ample resources, planned redundancies, security posture, knowledgeable/skilled staff, asset classification and risk profiling, and, governance, leadership and compliance. The eight constructs form the independent variables that are believed to have a cause-effect on the strength of cyber-resilience, the dependent variable.

Each of the constructs consists of a set of metric variables relevant to the business case and operating environment for Kenyan banks. The metric variables form part of the survey instrument whose purpose is to measure the cyber-resilience of each participating bank. The clustering of these metric variables is shown in Appendix C.



### 1.14.1 Conceptual Framework Diagram

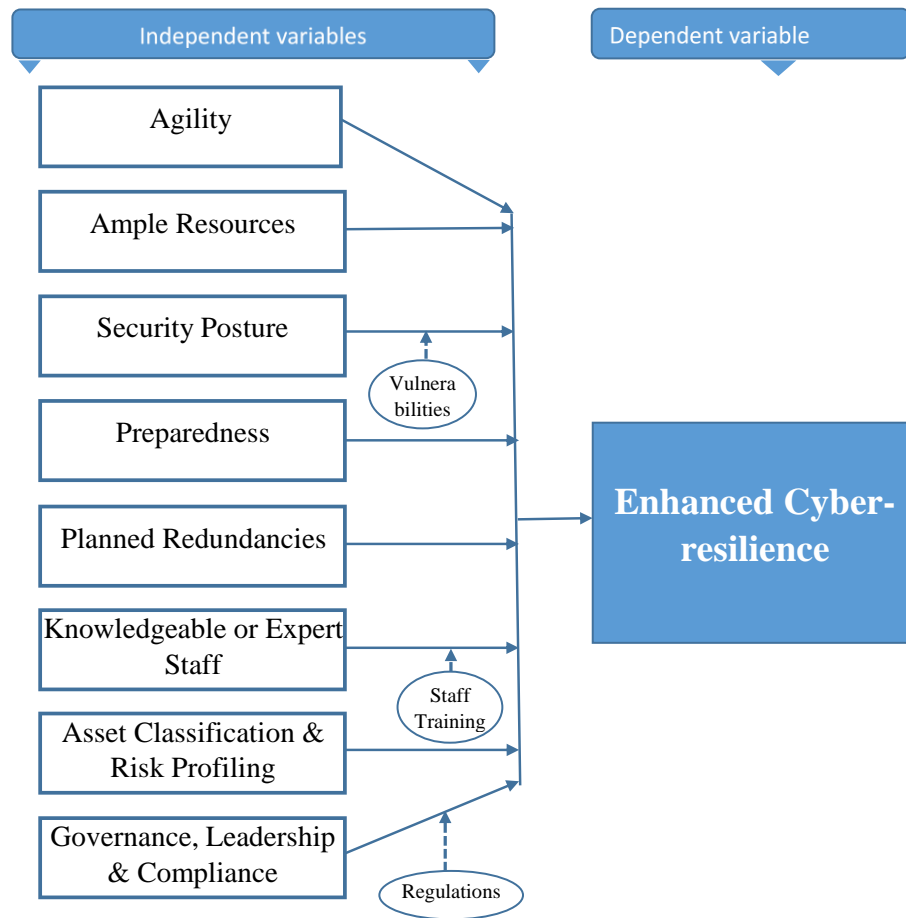


Figure 1-5: Conceptual Framework Diagram

The Conceptual framework diagram (figure 1-5) visualizes the framework defined earlier in section 1.1.4. It shows the eight variable constructs framed here as the independent variables and on whose basis cyber-resilience will be measured. The conceptual framework has modelled enhanced cyber-resilience as an object (dependent variable) dependent on several constructs (independent variables). Hence, an improvement or deterioration in the independent variables (constructs) should have an effect on cyber-resilience. The level of impact each has on cyber-resilience will be measured via statistical methods. Moderating the dependent and independent variables are: vulnerabilities and risks, existing legal framework, staff awareness and technical training. The constructs are elaborated further in section 2.4.2.

### 1.14.2 Conceptual Framework and hypotheses

In the diagram below (figure 1-6), the constructs have been transformed into eight hypotheses to help determine the level of cause-effects each has on cyber-resilience.

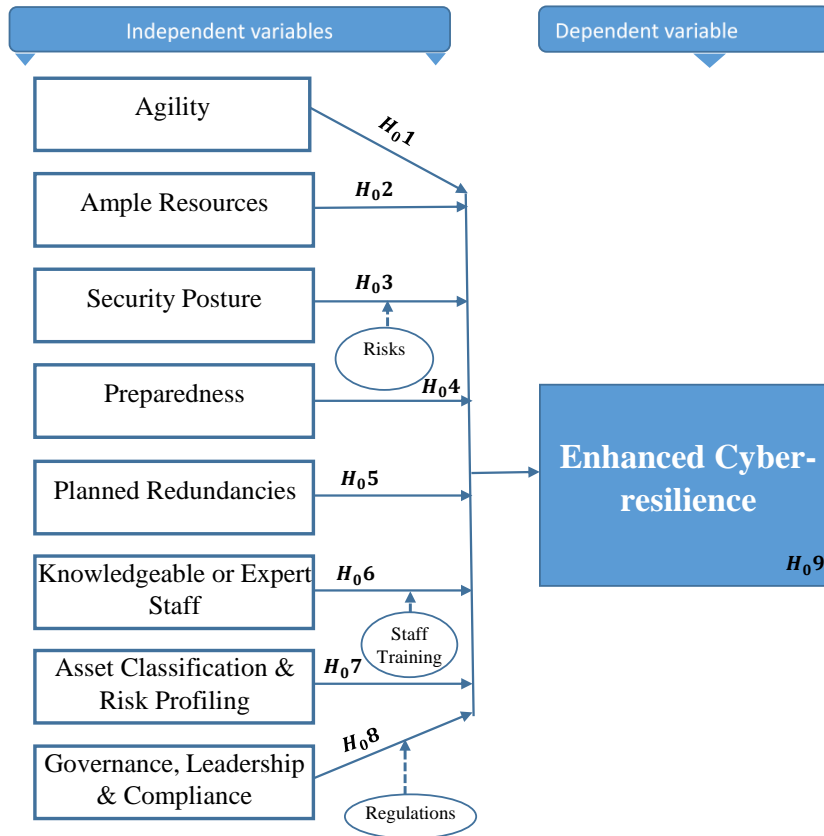


Figure 1-6: Relationship between Conceptual Framework Diagram and Hypotheses

## **CHAPTER TWO – LITERATURE REVIEW**

### **2.1 Introduction**

This chapter provides the breadth and depth of the theoretical and empirical arguments and counter-arguments aimed at either supporting the formulated hypothesis or discovering new ones. The chapter draws from different streams of cybersecurity and resilience literature (and also from non-ICT literature) and frameworks with a view to forming relevant building blocks for modeling a localized framework for measuring cyber-resilience in Kenya. Also in this chapter, we delve into details on variables necessary for designing the proposed cyber-resilience framework. The ultimate goal is to frame cyber-resilience as a characteristic of these variables, and to provide a universal foundation for measuring cyber resilience (Linkov & Kott, 2019).

### **2.2 Theoretical Review of Literature**

Although multiple metrics for quantifying various aspects of cyber resilience, have been published in some standards and literature, there is still no much unanimity and universality on which metrics suit specific situations, and it is posing a theoretical huddle (Antonucci, 2017, p.186). Some of the sources concentrate mainly on defining and operationalizing in depth cybersecurity. Sommestad, (2012) also suggest that although some of the publications describe the framework of how an organisation should develop and maintain a cyber-resilience assessment program, they do not define the actual measurements. Serianu (2015) suggests that Kenya needs to develop her own core cybersecurity and cyber-resilience philosophies, unique to the Kenyan ecosystem, instead of borrowing heavily from international best practices.

The new framework CRF4Banks anchors on Ponemon Institute's cyber-resilience framework. Not only does this association ensures reliability, it also ensures CRF4Banks benefits from multiple sources of tried and tested metrics.

### 2.3 Empirical Review of Literature

For a long time, organisations have focused mostly on cyber-defensive mechanisms in order to resist cyber-attacks. That gave birth to the commonly known practice of defence-in-depth. Resistance to cyber-attacks is undoubtedly a good strategy. However, when the laws of diminishing returns is applied, this strategy reaches an ineffective saturation point. It must be noted that resistance strategies employ mitigations that are mostly specific to a particular set of threats at point in time (Phil, 2016). Hence, any shift in attackers' strategies can easily bypass existing defences - and leave the organisation exposed to immeasurable downtimes and losses. Worse still, many organisation are not able to face up to the ferocity of nation-state attackers or state-sponsored cybercriminals. As such, cyber-resilience is the answer.

According to Department of Homeland Security (DHS), cyber-resilience helps to define the working space to help manouvre preparedness, agility and adaptability of an organisation to withstand the eventual occurrence of such disruptive threats or incidents. Effectively, cyber-resilience merges cybersecurity, the organisation, the organisation's systems and best practices. Hence, DHS strongly advocates for clear distinction between cyber security and cyber-resilience in order for each to get the attention it deserves.

Cyber-resilience has been a long way coming. It only got attention in the cyberspace domain as an offshoot of resilient business continuity programs (IBM, 2011). Then disaster recovery (DR) came in the mid-1990s paving way for business continuity (BC) and business resilience (BR). Conflating BC, BR with traditional techniques such as availability, recovery, security, resilience, and compliance, it has given rise to a strong infrastructure that drives a true business resilience programme (IBM, 2011). Thus, today, cyber-resilience has become a key element of a resilient business continuity programme.

When is an organization like a bank considered cyber-resilient? Antonucci (2017, p.186) reckons that there is no consensus on the criteria for determining a cyber-resilient organisation. North, Pascoe and Westgarth (2016) declare that cyber-security and resilience are all about governance and culture requiring everyone in the organization to participate – from employees and customers to the board of directors. North, et al. (2016) and Dhingra, et al. (2018) cite a seven-point strategy necessary to maintain true digital resilience in banks. First, by incorporating cybersecurity in

management and governance processes, which internalises cyber-resilience measures into business operational processes. Antonucci (2017, p.68) adds that any measures must be developed in the context of a cyber-security strategy that tightly connects with an organisation's overall business strategy. Second, by classifying and prioritizing information assets and their related risks. Further, strengthening cybersecurity protection for the key assets in the bank is also essential. Engaging the organisation's workers with cybersecurity awareness campaigns, incorporating security features into every IT system project are also important strategies recommended by Dhingra, et al. (2018). However, to eliminate complacency, Dhingra, et al. (2018), recommend deploying active defenses that regularly undergo assessment through simulations attacks, "war games" and penetration tests thereby increasing situation awareness and digital resilience.

Linkov and Kott (2019) posit that traditional cyber-risk assessment methods have focused on computations of threats, vulnerabilities and consequences for hazards, but with the advent of cyber-threats, these have proved limiting and unable to address threats and vulnerabilities that have become part of modern digitisation. Linkov and Kott (2019) add that for every equivalent growth in complexity of the interconnected systems, threats have also been innovating and evolving more rapidly than the approaches used to manage them. This call for innovative approaches beyond the traditional cyber security.

From a theoretical standpoint, the idea of modeling frameworks to address cyber-safety and cyber-resilience has been documented previously (Salim & Madnick, 2016; Antonucci, 2017). Kott and Linkov (2019) present two approaches that are popular in cyber-resilience literature. These are metric-based and model-based approaches. In fact, Caralli, et al. (2016) have detailed a holistic CERT Resilience Management Model (CERT-RMM) covering numerous resilience metrics.

### **2.3.1 Existing approaches to assessing Cyber-resilience**

#### **a) Ponemon Institute Research on Cyber Resilient Organisation**

Ponemon Institute has used its cyber-resilience instruments to conduct assessments in several organisations in United States, United Kingdom, France, Australia, Germany, Brazil and United Arab Emirates (2015; 2018, 2019). The

instrument is constructed upon seven factors termed as “The seven factors considered important in achieving a high level of cyber resilience”. These are preparedness, agility, strong security posture, knowledgeable or expert staff, leadership, preparedness, planned redundancies, and ample resources (Ponemon, 2018). These seven factors have been adopted into the new localized framework, CRF4Banks, with additions to form key variables.

#### **b) Serianu Cyber Security Framework**

Serianu Ltd. is a Kenyan-based IT services company that specializes in information (cyber) security services in Africa. Serianu regularly publishes researches on cybersecurity in Africa, chiefly “Cyber Security Report” for Africa, Kenya, Nigeria, Tanzania, Uganda and for SACCOs in Kenya (Serianu, 2015).

Serianu cyber security research studies are based on their own baseline controls, collectively known as the Serianu Cyber Security Framework (Serianu, 2015). Though built for regional suitability, the framework has incorporated best practices from COBIT, ISO 27001, SANS 20 Controls, and NIST. The Serianu Cyber Security Framework consolidates controls into four categories, namely: Cyber security programme governance and strategy, vulnerability and threat management, user provision and access management, and continuous monitoring and incident response (Serianu, 2015). As a result, this research benefits from both worlds of a localized framework incorporating international standards.

#### **c) Central Bank of Kenya Guidance Note on Cyber security (2017)**

The regulator of Kenyan banks, CBK, published guidelines for ensuring effective cybersecurity governance and risk management. The guidelines are divided into five domains viz. Governance, Training and awareness, Incident reporting, Risk management and assessment, and Outsourcing (CBK, 2017b).

#### **d) NIST- Framework for Improving Critical Infrastructure Cybersecurity v1.1**

Even though NIST describes this as not a one-size-fit-all framework, this framework was developed by NIST as a flexible way to address cybersecurity and its effect on entities using or not using IT - industrial control systems, or ordinary organisations (NIST, 2018). It groups the constructs into broader categories of Identify,

Protect, Detect, Respond and Recover. Each of these is broken down into twenty-one sub-categories, some of which (governance, compliance and risk management) have been coopted into the new framework of variables.

This research builds on these prior works and defines a framework consisting of an instrument for assessing cyber-resilience of Kenyan banks.

### **2.3.2 Constructs for measuring cyber-resilience.**

The eight constructs for measuring cyber-resilience will form the anchor criteria for the instrument's independent variables with amendments. Besides the seven dimensions used by Ponemon (2018), an additional dimension for asset classification and risk management, has been added from the CERT-RMM and NIST frameworks. To ensure that "governance and leadership" is more elaborated, compliance from CERT-RMM has also been appended. Altogether, there are eight parametric constructs in this instrument for measuring cyber-resilience in Kenyan banks. These are shown in Table 2-1 below. The questions in the research instrument have been modelled around these constructs.

### **2.4 Selection of metrics for measuring Cyber-resilience in Banks.**

Building metrics for cyber-resilience for a general organisation can be daunting (Dalziell & McManus, 2008). This research narrowed its study to a more structured and regulated sector as that of banks. Similarly, due to uniqueness and complexity of operating environment, organisations may experience threat impacts at different scales, while others may view a specific threat with an opportunity lens. To set a level-playing field and to ensure objectivity to the participants, the research elected to sample participants from banking institutions only.

**Table 2-1: Constructs for measuring cyber-resilience.**

<b>Construct</b>
1. Agility
2. Preparedness
3. Redundancy planning
4. Strong security posture

- 
5. Knowledgeable and expert staff
  6. Ample resources
  7. Governance, leadership and compliance
  8. Asset classification and risk management
- 

Source: Ponemon Institute, 2018, Literature review.

### **i. Agility**

While describing an agile framework, Worley, Williams and Lawler(2014) define agility as the ability of an institution to make timely, effective and sustained response to a changing circumstance (moving target), in a manner that helps sense threats and opportunities, solve problems and change the organisation's resource base. Clearly, from this description, a resilient bank would be flexible enough to reserve resources to help it maneuver when handling emergency cybersecurity incidents. Luers et al. (2003), Dalziell and McManus (2008) agree that this adaptive capacity enables an institution to modify its circumstances to move to a less vulnerable condition or back to the original state before the vulnerability, by reconfiguring their systems to maximize survivability during a sudden attack. Hence, agility is also about maneuverability and adaptability as enshrined in Darwinian theories that assert that species must adapt or perish.

Thus, achieving resilience or cyber-resilience can viewed in relation to vulnerability and adaptive capacity (Comfort, et al., 2010). From the diagram below (Figure 1-1), making a system less vulnerable and increasing its adaptive capacity increases its resilience. The diagram indicates that the system's adaptive capacity is tilting the equilibrium upwards in order to offset the downward pressures exerted by vulnerabilities. In so doing, resilience is maintained or improved.

### **ii. Preparedness**

Preparedness defines the readiness of a bank to respond to a cyber-threat or incident. It covers a number of processes including incident response, resource mobilization, crime scene and evidence preservation, post-incident communication and post-incident review. A modern information security programme must have capabilities to respond to cyber incident emergencies in an effective manner (Miora, Kabay &



Cowens, 2014, p56.2). This is because cyber threats have increased in intensity, approach and impact owing to increased emersion in digitisation. One of the ways many organisations, and indeed many countries have propped up their preparedness by forming CSIRT teams. A CSIRT team consists of multi-domain skilled personnel whose role is solely for emergency response (Rudolf, 2014, p. 56-3). More often, such teams also serve other roles such as running security awareness programmes, monitoring and other roles that complement preparedness of an organisation. According to a study on the cost of data breach, conducted by Ponemon (2018b) on behalf of IBM, availability of a incident-response team increases the efficiency in identifying an incident and the speed of the response, hence, significantly lowers the cost of a breach.

### **iii. Redundancy planning**

Redundancy planning incorporates all functions of business continuity and contingency processes. According to Cabarello (2009), business continuity and contingency planning ensure that critical functions in a business can withstand a disaster. A cyber-resilient organisation is one that successfully aligns its continuity management and disaster recovery into an elaborate in-house business continuity plan (Ponemon, 2018).

According to Miora (2014), maintaining redundancy requires that an organisation duplicates facilities, infrastructure and sometime roles across multiple geographic locations, and also, test the systems for breakdown scenarios. Redundancies planning also incorporates escalation timelines (Miora, p.59-3) that indicate classification of damages according to outage duration and scope of effects.

### **iv. Strong security posture**

Strong security posture is a combination of multiple implementation factors. Mallery (2009, p.3-21) provides ten practices that ensure a “robust” cyber-security posture. First, a bank needs to evaluate and rationalize the risks and threats around each asset. Second, the bank needs to provide cybersecurity training for IT staff and general staff; strengthen security of operating systems and applications used in the bank; procure and install elaborate cybersecurity tools for monitoring systems in the bank; develop and utilize internal security audit functions, augmented by third-party support.

Mallery (2009, p. 18) prefers contracting external professionals because they have experience reviewing a wide range of systems. Lastly, implementation of principle of defense in depth ensures layered security mechanisms that increase systems security as a whole. This approach requires what Caballero (2009) calls “ground up” concept, which entails handling information security from the physical layer, working your way up to the top (application) layer, effecting total security. The objective is to ensure that every possible vulnerability point is covered layer by layer.

Strong security posture also involves incorporating technologically advance functions such machine learning and automated network defense mechanism.

**v. Knowledgeable and expert staff**

This construct deals with training of staff in cybersecurity awareness, and in essential skills required to defend the bank from cyber-attacks. Many organisations have concentrated on staff awareness because it is a well-known fact that staff are the weakest point in the vulnerability security-chain. According to NIST Special Publication 800-16 Revision 1, security awareness and role-based training applies to all employees regardless of whether they use or interact with information systems or data. An effective security awareness program should be enriched with latest security information and inculcated from recruitment time and be refreshed periodically (Rudolph, 2014, p. 49.3-49.4) because cybersecurity risks and vulnerabilities evolve continuously. Besides enforcing a mandatory internalized training curriculum, some organisations go further by requirement staff to attest their responsibility by signing that they understand what the training is demanding them to learn (Rudolph, 2014, p49.10).

**vi. Ample resources**

Successfully mitigation and eventual thwarting of attacks requires an organisation to have enough resources that can handle sustained attacks (Noble, 2009, pp.693-700). Sometimes this can mean redundant sites for offloading the attack. Ampleness and diversity in resources may have considerable cost but may in fact help support other systems and decision makers to have immediate options during a sustained attack (Noble, 2009, p694).

### **vii. Governance, leadership and compliance**

North, et al. (2016) decry that many bank boards may still be burying their heads in the sand when it comes to cybersecurity and cyber-resilience measures. Today cybersecurity is a major governance issue, and always featuring on management agenda. This, according to North, et al. (2016) has been necessitated by huge losses caused by cyber losses, or because of too much bureaucracy that slows down corporations from reacting fast to incidents. NIST Cybersecurity Framework defines five functions that must be coopted – functions which will form the backbone of this research. These are identification of and protecting assets, detecting, responding and recover from attacks.

### **viii. Asset classification and risk management**

The purpose of this construct is to rationalise and classify assets based on their importance, value, risk and criticality to the operations of the bank, and then allocate cybersecurity resources to the assets appropriately (Mallery, 2009). Without understanding the value of an asset and the risks it attracts, it becomes difficult to prioritise protection required. Some assets require more resources than others.

## **2.5 Research Gap**

It is evident from the foregoing literature review that cyber-resilience has been gaining traction in many institutions across the globe. This is supported by Ponemon Insitute's latest report on cyber-resilience (Ponemon, 2019) which indicates that the number of organisations embracing the value of cyber-resilience has been growing steadily but slowly from 51% in 2016 to 65% in 2017, and 62% in 2018. In the same report, cyber-resilience increased from 32% in 2016, to 48% in 2017, and 54% in 2018. While many research studies such as those done by Ponemon Institute have demonstrated that it is possible to build a successful cyber-resilience, what is lacking is unanimity on what content it should contain to satisfactorily measure cyber-resilience (Kott and Linkov (2019, p.10). Moreover, the widely used Ponemon Institute framework omits some essential variables such asset classification and risk profiling, governance and compliance. Banks are exposed to unique risks, yet none of the literature reviewed has a specific framework for assessing cyber-resilience of banks. The risks that banks CERT-RMM and NIST frameworks are very voluminous in the number of metrics they cover, yet too general to be suited for a banking institution. This

calls for a need to customized the frameworks to fit the unique circumstances of the banks (Shapiro & Keys, 2019, p.73).

## **2.6 Summary of literature review**

Although multiple metrics have been proposed for quantifying various aspects of cyber resilience, a link should be made between those metrics with those which are operationally measurable and relevant to cyber-resilience (Kott and Linkov, 2019, p.17). Appendix Table B-1 provides the instrument developed out the literature review and previous works.

## **CHAPTER THREE – RESEARCH DESIGN AND METHODOLOGY**

### **3.1 Introduction**

This chapter describes the research design and the methodologies employed in this research. It concentrates on the design of methods used to fulfil the objectives defined in chapter one. In a nutshell, the objective of the research is to develop a localized cyber-resilience framework and use it to assess the cyber-resilience of Kenyan banks. Cyber-resilience has been gaining traction but lacks methods of quantification. The chapter utilizes the new framework conceptualised in chapter two to define the instrument used in assessing cyber-resilience in banks. The instrument, as observed, consists of eight constructs forming key categories for the metric variables that have been used in the instrument to quantify cyber-resilience. They include agility, preparedness, redundancy planning, strong security posture, knowledgeable and expert staff, ample resources, governance, leadership and compliance, and asset classification and risk management.

The chapter covers an enumeration of the background of the research design, gap in research, details about the research instrument, research plan, targeted group, sampling method, process of collection of data and results of the pilot study. Data analysis design and the choice of data analysis methods to be used in chapter four are also documented.

### **3.2 Research Design**

According to Kumar (2011), a research design serves two purposes, first, to identify and develop procedures and logistical processes required to undertake a study, and second, to emphasise the importance of quality in the processes ranging from ensuring validity, objectivity, accuracy and ethics.

The literature review curved out some grey areas found wanting in the adopted framework for Ponemon, but which were well documented in a mix of other standards and models. This incorporated addition of Asset classification and risk management as a new construct and the widening of Leadership construct to include Governance and Compliance – key measures that are recommended by NIST and CERT-RMM

frameworks. The eight constructs form the basis of the key areas of measuring cyber-resilience. Each construct will consist of a set of metric variables. The variables describe situations, feelings, perceptions, attitudes, values, beliefs and experiences of people. The research study has used quantitative methods to measure the variables.

The instrument for the research study is a self-administered questionnaire. The questionnaire is shown in Appendix B. It consists of a series of close-ended questions.

### **3.2.1 Research Plan**

This research was be divided into three phases:

#### **Phase 1: Development and construction work**

This first phase involved re-modelling the variables into a suitable questionnaire for data collection. This involved adding context-specific variables while also removing irrelevant variables to ensure that the framework comprehensively captured elements relevant to Kenyan operating environment, and to maintain fidelity of the evaluation to acceptable international standards. The completed instrument then underwent two validation processes before being deployed in the main research:

- i) First, the instrument was subjected to scrutiny, through an expert review consisting of African Nazarene University faculty and then externally from domain experts.
- ii) The questionnaire was deployed into a pilot testing with a small sample of 3 Cooperative societies and 1 bank.

Once validation of the questionnaire was completed, the expected output from Phase 1 was a validated questionnaire.

#### **Phase 2: Large-scale application**

During this phase, the developed survey instrument was deployed to the targeted population decided through random sampling method. The instrument was delivered to the respondents using email and self-administered using online questionnaire hosted on Survey Monkey.

### **Phase 3: Tabulation and Validation of the result**

Data collected from this phase was tabulated, validated and cleaned. Cronbach Alpha was used to evaluate the validity of the data. Additional descriptive statistics methods were also employed.

#### **3.2.3 Framework and Research Instruments**

Producing credible cyber-resilience research on banks in Kenya and indeed elsewhere requires approaches beyond rudimentary. The methodology must not only be reliable and credible but also tried, tested and of highly confidential nature. To this end, a new set of variables (found in Appendix B-1) for cyber-resilience was developed from literature review and studies done by Ponemon Institute, Serianu, and Symantec. The variables have been customised for the Kenyan environment. Whereas the Ponemon research sampled a wider and mixed corporate environment, this research will however, be restricted to a sample frame of forty-five banks and mortgage institutions in Kenya. A representative sample of banks to participate in the survey will be derived using random sampling technique.

Due to project time constraints and the difficulty of reaching the targeted respondents in the banks, this research elected to use a self-administered questionnaire as the data collection instrument. Appendix Table B-1 shows the questionnaire developed for this purpose.

One of the salient features of the questionnaire is that it did not include information that positively identifies a respondent and his/her bank. Hence, during data collection, the questionnaires did not have names identifying respondents or their institutions. However, after the forms were returned, they were coded to facilitate easy reference during analysis.

### **3.3 Research Site**

The research was conducted at the head office of the banks in Kenya. All banks in Kenya have head offices in Nairobi, according to information from KBA. Consequently, this research was conducted in Nairobi County. The map of the coverage area can be seen in Appendix E.

### **3.4 Target Population**

The research will target Kenya's regulated banks and mortgage institutions, both for the main research and the pilot-testing. Financial institutions such as mobile money

transfer operators, Saccos, micro finance institutions, and payment intermediaries have been excluded in this study because they are not members of KBA, but could be viable candidates for this study in future.

There are 47 commercial banks (including one mortgage company) in Kenya, according to the Kenya Bankers Association data (Kenya Bankers Association, 2019). Three of the banks were excluded from the sampling frame because they were in receivership. The research sampling frame therefore consisted of a homogenous finite population of 44 banks, giving a population value (N) as 44. Due to project time constraints, a sample size was extracted from the list of 44 operating banks using simple random sampling formula by Cochran's (1963). Each sampled bank provided one respondent person to complete the questionnaire.

### **3.5 Determination of Research Sample Size**

#### **3.5.1 Sampling Procedure**

Out of the 44 banks operating in Kenya, a random sample research size was computed and used in this research. According to Zikmund, Babin, Carr and Griffin (2009), it is not necessary to take a census of all banks in the sample space to achieve accurate study. As one of the commonly used methods, simple random sampling was used as it accords equal and independent sampling opportunity to each member of the targeted population (Zikmund, Babin, Carr, and Griffin, 2009), and is deemed as a suitable method by Sekaran and Bougie (2009) to conduct a research whose outcome is expected to be generalized, in this case, to all banks in Kenya.

#### **3.5.2 Study Sample Size**

In this research, the Cochran's formula (1963) was used to compute the research sample. The Cochran formula provides one of the ideal methods for deriving a sample size when provided with confidence level, margin of error and a finite representative population, N. The formula uses three important values: population size (N), representing the numbers of in the sample frame, which is 44; the margin of error, a percentage value that shows how far the survey results deviate from that of the full population; assumed margin of error of 5%, which gives a confidence level of 95%. Confidence level is expressed in percentage or decimal, and provides a probability that the results will be reliable and hold true to the population sampled, and 95% has been



used widely by researchers according to Zikmund, Babin, Carr, and Griffin (2009, p.430). The Cochran formula is stated thus.

$$n_0 = \frac{Z^2 pq}{e^2} \quad (3.1)$$

Where  $n_0$  = the sample that we want to derive and use in the research;

$Z$  = is the z-value from standard graphs representing 95% confidence level, which is 1.96;

$e$ =margin of error – the level of precision, which is 5% and with level of confidence of 95%;

$p$  = is the estimated proportion of an attribute that is present in the population, i.e. 0.5, and  $q$  is  $1-p$ .

Applying equation (3.1) for a large population this translates to :

$$n_0 = \frac{Z^2 pq}{e^2} = \frac{(1.96^2)(0.5)(1 - 0.5)}{(0.05)^2} \approx 385$$

Next is to apply the formula for finite population (with  $N=44$ ) correction factor, which aims to adjust the computed sample  $n_0$ .

$$n = \frac{n_0}{1 + \frac{n_0 - 1}{N}} \quad (3.2)$$

Hence the sample size for our research  $n$  is derived by applying equation (3.2) as below:

$$n = \frac{385}{1 + \frac{(385 - 1)}{44}} \approx 40$$

Consequently, the sample population for this study consisted of 40 banks chosen randomly.

### 3.5.3 Sample Selection

The full list of the 47 banks comes from Kenya Bankers Association website (2019). Three banks in receivership were removed from the list, leaving 44 banks for the sample frame.

The 44 banks were enlisted as ordered in the original list. Before sampling out the 40 banks for the research, the natural list was randomized. Using an automatic sample generator software known as Research Sampler. Next, the new randomized list was given a sampling number ordered from 1 to 44 (from top to bottom). The list was then sorted in ascending order, giving an ordered population set of banks  $N\{1, 2, \dots, 44\}$ . The order was then input into the Research Sampler to extract a random sample of 40 banks. After the sampling, four banks were dropped out by the sampling program. Finally, the new list of the remaining 40 banks was provided with new sequential numbers to act as research codes. Table E-1 shows the sampled list of 40 banks.

The distribution of the sampled banks against the total population, classified according to CBK's peer size, is shown in table 3-1.

**Table 3-1 Sample Size Distribution by peer size**

<b>Peer Size</b>	<b>Small</b>	<b>Medium</b>	<b>Large</b>	<b>Total</b>
Sampled banks	21	13	6	40
<b>Total bank population</b>	24	14	6	44

### **3.6 Target Respondents**

Antonucci (2017) advises on the use of multiple participants when researching in each sampled organisation. This is because, apart from providing granularity and reducing respondents' individual biases, it also adds variations in responses that tend to enrich a discussion about different assumptions and practices. In this research, however, the number of participants per banks was one. The expected respondent demographic profile would be senior staff in charge of or are accountable to all aspects of cybersecurity and/or cyber-risk, and who possess broader understanding of the overall objectives and practices of the bank's cybersecurity. This could be Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Risk Officer (CRO) or any other person managing this role.

### **3.7 Sampling Design**

Two samples were formulated: the main research sample and the pilot-test sample.

- i) Main Research Sample.

As mentioned in the Target Population section, the main research targeted the sample size  $n=40$  out of a fully active bank population of 44.

ii) Pilot test Sample.

Pilot testing for the research questionnaire, a sample of six ( $n=4$ ) non-participating financial institutions were purposively selected to participate, i.e, one from deposit-taking Cooperative Societies, one from deposit-taking Microfinance institutions, one from Mortgage firms and one Commercial bank.

Feedback from the test-survey and review by the faculty on the research instrument necessitated further revisions to the variables and the instrument itself. Types of specific feedback sought from this advance survey included question clarity, relevance, suggestions for rewording, and examples of specific behaviours brought to mind in the rating of each variable. Other important feedback were adapted from Bell (1987). Participants were asked to provide any additional comments that they consider relevant. This trial was conducted face-to-face, so that the feedback can be collected easily. Changes to the survey instruments were then made on the basis of this feedback.

### **3.8 Variables and Constructs**

The structure of the research instrument consists of several questions grouped into eight constructs designed to measure specific attribute or characteristics of the cyber-resilience. There are eight constructs adopted in this research as shown in section 2.3.2.

#### **3.8.1. Measuring and grading constructs**

Each metric variable is presented to the respondent as a question. Multiple Likert scales and multiple response questions have been used. Each response has a numeric value based on a scale. The value of each response enumerates a unit characteristic of cyber-resilience strength under one of the eight constructs of cyber-resilience. The weighted mean was computed for the response values. These responses were recoded into a composite 5-level Likert scale representing the cyber-resilience strength 1 to 5 as shown in Table 3-2.

**Table 3-2: Ranking and grading scheme for cyber-resilience**

Grading	Weighted Mean score	Grading ranking strength
Very weak	$\leq 1$	1
Weak	$> 1$ and $\leq 2$	2
Moderate	$> 2$ and $\leq 3$	3
Strong	$> 3$ and $\leq 4$	4
Very strong	$> 4$ and $\leq 5$	5

Some responses have two or three choices. Where the responses are two or even number, the midpoint in the 5-scale will not be used. The extreme scale values will be used. For example, in a forced “Yes” or “No” answer, the “Yes” or “No” may be re-coded to be Very Strong or Very Weak depending on the survey question. By aggregating all the responses using this 5-level scale, it is possible to compute the score per respondent. The scale is from 1 to 5, with 1 denoting “Very Weak”, 2 as “Weak”, 3 being “Moderate”, 4 as “Strong” and lastly 5 as “Very Strong”.

**a) Grade 5 - Very Strong**

Grade 5 is the highest level. A score of grade 5 is designated as very strong in cyber-resilience stature. They are highly adaptable, have invested a lot resources in cybersecurity, has dedicate personnel and utilizes the strength outsourced services to strengthen its capacity. An organisation at this stature has deepened risk assessment, never complacent and continuously evolving it defences to beat vulnerabilities. More important, is the ability to sustain any attack because of huge investments in automated redundancies and disaster recover processes.

**b) Grade 4 - Strong**

Grade 4 symbolises strong statures. Closely related to level 5. However, occasionally, cyber attacks may filter through. When such happens, organisations at this level have mechanisms to ensure minimal disruption. They employ highly skilled staff to maintain different aspects of cyber-resilience.

**c) Grade 3 - Moderate**

A moderately-graded bank is one that has put in place all the necessary systems. However, they are very vulnerable, unpredictable and unstable if attacks were to happen. Recoverability from an attack may take a few hours.

**d) Grade 2 - Weak**

An organisation at this state has weak systems, processes and skills that cannot sustain an attack. Downtimes are frequent and repeat attacks may occur. This is a risky state to operate a business, no more than a banking institution.

**e) Grade 1 - Very Weak**

Grade 1 is the lowest status. It points to a total lack of systems to secure an organisation from cyber-attacks, and mechanisms to recover from them. There is disjointed management of cybersecurity, and vulnerabilities are always lurking. There are no specialized staff to manage cybersecurity. Staff may not be aware of their role in combating incidents, neither is there enforcement.

**3.8.2. Demographic variables**

In this research study, a number of questions are for gathering demographic information. They help to characterize the target client according their natural group. These include peer size (small bank, medium bank and large bank). The regulator does the classification by peer size. Other demographic information include budget size, total staff count, size of IT department, size of the IT security department and size of budgets allocated to IT department.

**3.9 Data Collection measures**

The data collection instrument adopted for this research was an online questionnaire delivered through Survey Monkey. The reason for using the questionnaire as a tool is due to the number of questions involved and the short time required to complete the research.

The SurveyMonkey link to the questionnaire was distributed to the respondents electronically using email containing both the URL and QR code for mobile devices. Only pilot-run questionnaires were delivered in hard copy. The online survey was especially helpful in reducing the cost of the research (Sekaran & Bougie, 2009). Each

bank was provided with a unique URL link to the survey. The survey URL link contained an allocated research code encoded with md5 encryption to prevent obvious identification of the bank it belongs to. For hard copy questionnaires, the collected data was input into the online questionnaires.

### **3.9.1 Question types**

The questionnaire has closed-ended questions in the form of multiple choice check-boxed types, single-choice radio buttons, and matrix questions composed of a mix of four, five and seven Likert scale choices. Checklist questions allowed a respondent to select multiple answers for a question (Zikmund, Babin, Carr and Griffin, 2009, p.341). Such types of choices were added as individual variables.

### **3.9.2 Distributing the instrument**

The research was approved by NACOSTI on February 1, 2019 vide permit number NACOSTI/P/19/20367/27925 (see Appendix Figure F-2). Distribution of the instrument and collection of data for the main research started on February 21, 2019 and ended on March 31, 2019. Survey Monkey provides a mechanism to send a research to a mailing list. In this research, 40 Survey Monkey ‘collectors’ were created representing unique survey URL for each of the sampled banks. The URLs were distributed to each individual bank, confidentially through the bank’s provided contact email address. Distribution of the instrument for pilot testing was, however, done as manual questionnaires.

### **3.9.3 Matters arising from the Pilot Study.**

The pilot study, though had fewer participants (n=4), provided invaluable feedback that necessitated changes into the main research. With a Cronbach alpha  $\alpha$  coefficient of .89, the instrument appeared credible as it exceeded the recommended Cronbach alpha  $\alpha$  of .7 recommended by many researchers (Kothari, 2004). Even though the pilot study findings were not used in the final analysis a few observations were applied:

1. The sampling method for the population changed from census to simple random sampling due to the difficult in accessing the institutions, and their privacy procedures. In a research conducted in Jordan (Nuseir, 2010), in which the response rate was accepted at 63.4%, banks were conservative in

giving access to researchers. Gordon (2016) also adds that online surveys attract lower response rates than face-to-face surveys. These informed the need to change from the census to sampling.

2. Respondents indicated that the questionnaire was very lengthy and detailed. Further adjustments were made and questions reduced to 56.
3. The pilot test noticed a pattern of uniform responses and non-responses for matrix questions, a sign that some respondents were replicating one response to others, without careful examination of the questions. Consequently, changes were made to ungroup and mix up the questions.
4. Additional response choices had to be added for “Any other- Please specify” and “None of the above” to provide flexibility.

### **3.9.4 Instrument Validity**

Validity of the questionnaire and scales used were evaluated by face validity and also by content validity.

Face validity ensures that the instrument measures what it is intended to measure, at a face value (Sekaran & Bougie, 2009). Regarding face validity, the instrument was presented to an academician and a cyber-security practitioner to review and recommend its appropriateness and objectivity, design look and feel, layout and content. Content validity, according to Sekaran and Bougie (2009) ensures that the instrument has representative items that measure the concepts or the specific domain in question, using the various cyber-resilience constructs. The instrument was also used in a pilot study, whose outcome was instrumental in re-designing the instrument for the main research.

### **3.9.5 Instrument Reliability**

Reliability of an instrument is a test of consistency of the instrument when used in other studies. It ensures that it would result into collection of the same data in repeat operations (Babbie (2007, p.143). Data collected with the questionnaire during the pilot study was measured using Cronbach Alpha  $\alpha$  coefficient. Mugenda and Mugenda (2003) recommends that a reliable instrument should have a Cronbach Alpha  $\alpha$  coefficient value of at least 0.7.

### **3.10 Ethical Considerations**

Banks are very sensitive about data disclosure. Therefore, appropriate ethical measures were put in place to instill confidence. First, the research instruments bore no names or codes identifying participants. Secondly, the researcher sought approval from Africa Nazarene University, NACOSTI, the CBK and the KBA. Additionally, no form of financial aid or support was solicited from the regulators of the targeted institutions. Furthermore, the online tool, SurveyMonkey, was also configured not to store IP addresses of respondent computers. Finally, no reference to individual institutions will be made in any reports or publications produced on basis of the study results.

### **3.11 Data Analysis Design**

The ultimate aim of the research is to development a measurement instrument for cyber-resilience, and then deploy the instrument in a research study of Kenyan banks. The design of the data analysis was such that the questions in the instrument would be summarised into the eight construct categories. Each question's response was recoded at the construct level into a five-point Likert scale ranking (table 3-2) representing cyber-resilience strength.

Step 1: Response data is cleaned up. This involved setting null values to zero to indicate "Not selected".

Step 2: Each response ranked as indicated.

Step 3: Aggregating weighted mean measure and ranking each constructs. The result is a ranking per construct, but also available per bank and per question.

### **3.12 Data Analysis methods and tools**

The research has used a number of analysis tools and statistical analysis methods. The choice of the methods depended on their appropriateness to help prove or answer some perceptions or support a conclusion. These include:

#### **3.12.1 Analysis tools**

Three tools were used to analyse and aggregate the data. These are: Survey Monkey which provided its data collection and analysis capabilities, IBM SPSS and Microsoft Excel, both used analyse the data and draw graphs.



### **3.12.2 Measures of Central Tendency**

These include descriptive statistics such as mean, weighted mean, median, and mode were used widely in this research. Analysis of the relationships between these were also attempted and interpretations provided.

### **3.12.3 Measures of association or relationship measures.**

Models such as correlation and regression have been used. The degree of variability or association between variables was assessed by correlation coefficients and p-value. The linear regression model is  $Y = a + bX + e$ , where  $a$  is intercept,  $b$  is the slope of the regression line and  $e$  is error term. This equation was used to predict the value of target variable based on given predictor variable(s). The coefficient of determination,  $R^2$  was used to determine proportion of variance.

### **3.12.4 Pearson's Correlation Coefficient (r).**

The Pearson Correlation coefficient (r) was used to determine the strength and direction of relationship between variables. The data will be generated from SPSS.

### **3.12.5 One-way Analysis of variance (ANOVA)**

ANOVA has been used to measure differences between means and to conduct hypothesis testing for each of nine null hypotheses – and to determine whether to accept or reject them. ANOVA computation is to be done and output using SPSS. A typical ANOVA analysis summary table will look as below:

Source of Variation	Sums of Squares (SS)	Degrees of freedom (df)	Mean Squares (MS)	F-ratio
Between samples /categories	$SS_B = \sum n_j(\bar{X}_j - \bar{X})^2$	$df1 = k - 1$	$MS_B = \frac{SS_B}{k - 1}$	$F = \frac{MS_B}{MS_E}$
Residual (or Error)	$SS_E = \sum \sum (X - \bar{X}_j)^2$	$df2 = N - k$	$MS_E = \frac{MS_E}{N - k}$	
Total	$SS_T = \sum \sum (X - \bar{X})^2$	$N - 1$		

Where

- $X$  = individual observation
- $\bar{X}_j$  = sample mean of the jth sample (or group),
- $\bar{X}$  = overall sample mean,
- $k$  = the number of samples or independent comparison groups, and
- $N$  = total number of observations or total sample size.
- $SS_B$  = Sum of squares between groups
- $SS_E$  = Sum of squares within groups (error)
- $SS_T$  = Sum of Squares Total
- $MS_B$  = Mean Squares between group
- $MS_E$  = Mean Squares within groups (error)

### 3.12.6 Using one-way ANOVA to test for Hypothesis

1. First, obtain the F-value (F-ratio) from the ANOVA table output above.
2. Taking the degree of freedom  $df(df1, df2)$  and research's significance level of 0.05, derived, from the F-distribution table, the critical-F.
3. Test for hypothesis: if F-ratio (computed from the summary) value is greater than F-critical, the null hypothesis will be rejected. Consequently, alternate hypothesis will be adopted.

## CHAPTER FOUR – RESULTS AND ANALYSIS

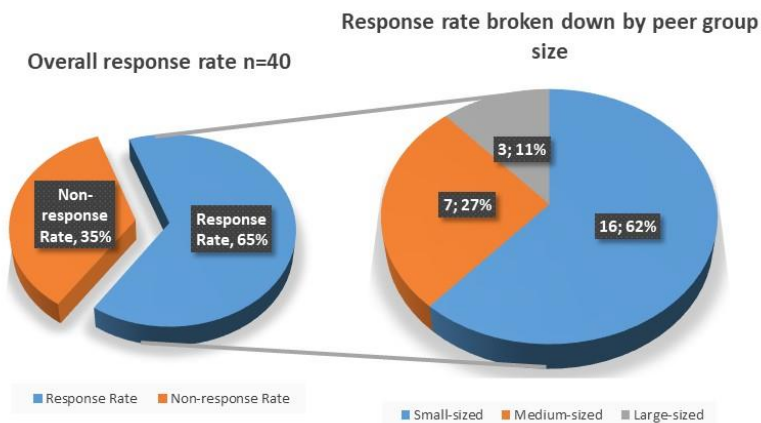
### 4.1 Introduction

This chapter presents the results and analysis of the research study. It is organized into five sections of Introduction, Response rate, Presentation of findings, Test of hypotheses and overall Cyber-resilience scoring. The chapter presents the results using both descriptive and inferential statistical methods. Deductions are also derived. Results are presented in tables, graphs and in descriptions.

The research objective first sought to collate cyber-resilience measurement variables from previous research works and standards and develop these into a new framework for assessing cyber-resilience of Kenyan banks. It then used the instrument developed from the framework to assess the cyber-resilience posture of banks. The assessment, in form of a survey, also acted as a way of validating the framework's instrument. The outcome is presented in the sections that follow.

### 4.2 Response Rate

A total of 40 online questionnaire links were dispatched to 40 cybersecurity accountable staff in 40 banks, one for each bank. Out of the 40 sampled respondents, only 26 filled and returned their questionnaires. The result is a 65% response rate as depicted in Fig 4-1. The questionnaire had 56 questions whose completion time averaged 17 minutes 59 seconds (for the 26 respondents) according to Survey Monkey online statistics.



**Figure 4-1: Overall Response rate for n=40**

Convincing banks in Kenya to participate in a research was one of the most challenging tasks. Many banks would not participate, fearing disclosure of sensitive information. Out of the 26 respondents, only two completed the questionnaires without repeat callbacks. The fact that 92% of the surveyed respondents only managed to complete the questionnaire after callbacks is an indication of the challenges that threatened the validity of the research during data collection. Table 4.1 provides a summary of targeted population.

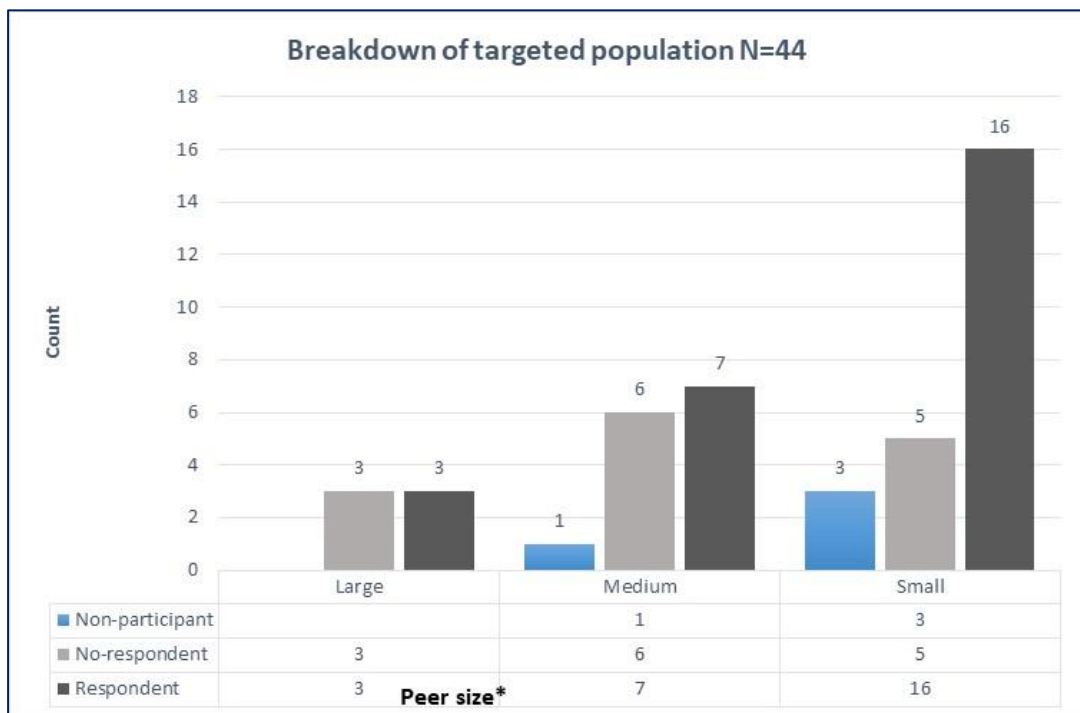
**Table 4-1: Response statistics**

Particulars	Representing	
Total Banks (Kenya Bankers Associating List)	47	Universe
Banks in receivership removed	3	6% of all banks
Banks available for Sample space	44	94% of all banks.
Sample population size by Cochran's formula	40	91% of sample space (n=40)
Number of questionnaires dispatched	40	
Number of questionnaires returned	26	65% of sample population
<i>Returned with zero call-backs</i>	2	2% of successful responders
<i>Returned with many call-backs and visits</i>	24	92% of successful responders
Total Non-responders	14	35% of sample population
<i>Direct refusals</i>	6	15% of sample population
<i>Non response</i>	8	20% of sample population

#### 4.3.1 Response Rate Validity

Babbie (2007, p.262) provides a discussion of acceptable research response rates, and suggests that there are no fixed written rules about it. While Gordon (2016) roots for a response rate of 50% to 60% (and lower values for online surveys, 25% to 30%), Babbie (2007) suggests that 60% is considered good while 70% or more is considered a very good completion rate.

This research takes the position that the 65% completion rate achieved in this research is adequate for the intended inferences. One of the reasons for this is that the population is representative of the small-medium-large classification by the CBK. Moreover, all these banks are regulated under the same parameters by the CBK. The analysis in Fig. 4-2 shows small banks as the majority of respondents (62%; N=16), followed by medium-sized (27%=7), and lastly, large-sized banks at 11% (N=3). Against sampled potential, 50% of large-size banks responded (3 out of 6); medium-sized at 54% (7 out of 13); small-sized banks at 76% (16 out of 21).



**Figure 4-2: Break-down of target population by peer group size**

### 4.3.2 Confirmation of Instrument Reliability

The targeted instrument reliability using Cronbach Alpha  $\alpha$  was 0.7, as per recommendations by Mugenda and Mugenda (2003). This research attained a Cronbach Alpha value of 0.73 during the main research and 0.89 during the pilot study, both surpassing the recommended value, and confirming the instrument reliability as shown in table 4-2a below.

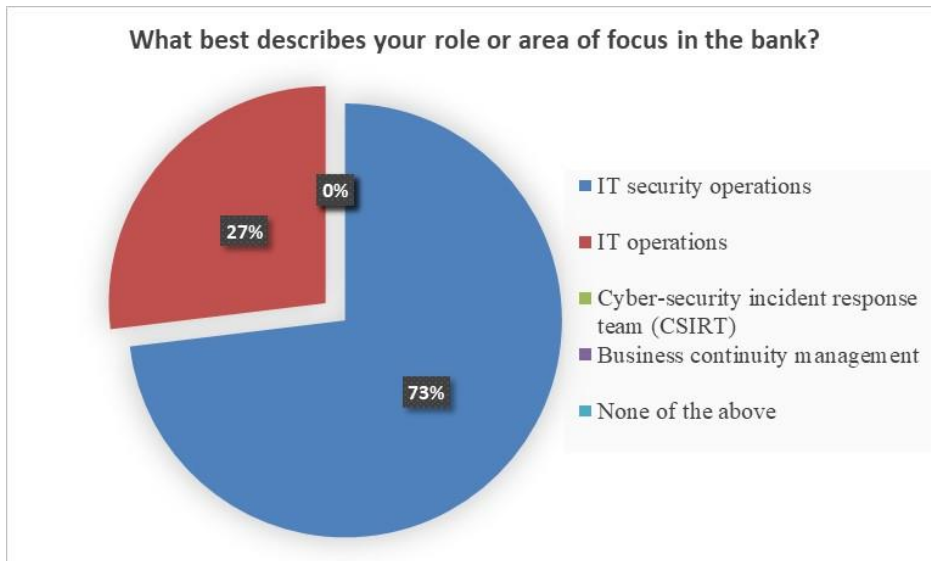
**Table 4-2a Comparing reliability statistics for the pilot study and main research instruments**

<b>(a)</b>			<b>(b)</b>		
<b>Pilot study</b>			<b>Main study</b>		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.890	.897	125	.727	.875	129

### 4.3 Presentation of findings

#### 4.3.1 Demographics and relevance of Respondents

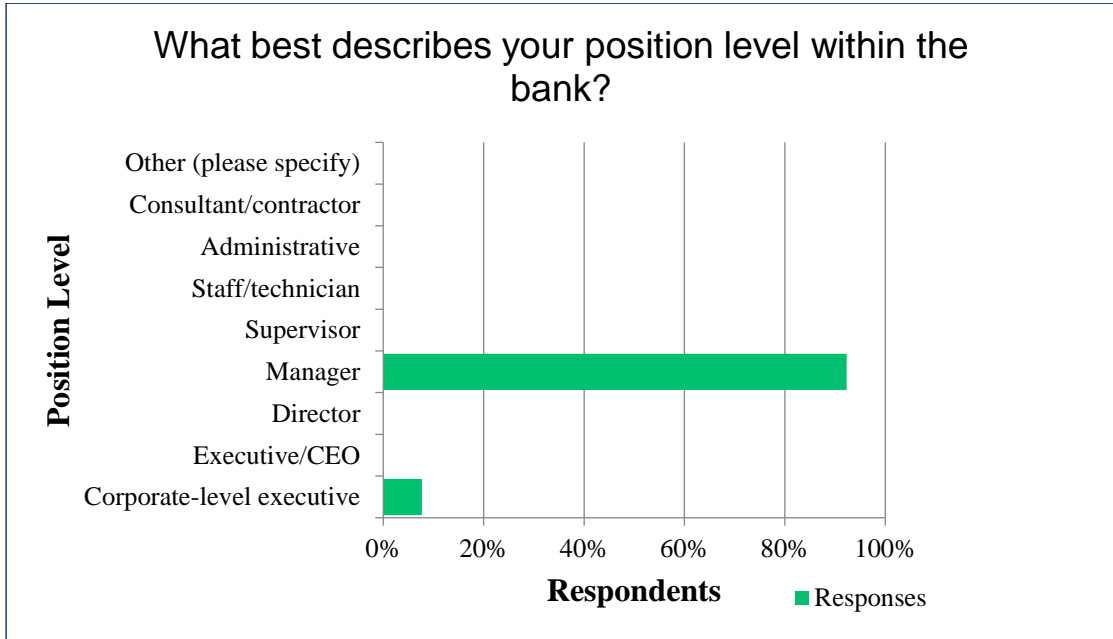
The questionnaire sought to confirm the suitability of the respondents as candidates for the survey through a series of demographic questions. The results depicted on figure 4-3 show that all the respondents (100%, n=73%+27%) were IT and IT security operatives based on their roles, and activities on the roles (as shown in Table 4-2b). This was important data because resource capacity, adequacy and expertise were essential measurements for understanding what influence they bear on capacity of banks to achieve cyber-resilience. It correlated well with data for the participants' position level (as shown in Figure 4-4 below), majority of whom were Managers (92.31%) and Executives (7.69%). The outcome of this met the conditions set out for the research, that required that respondents to be persons in charge of IT or cybersecurity in their organisations. Similarly, all the respondents (100%, n=26) were reportees to the CIO or Head of Corporate, COO or CEO (as shown in Figure. 4-5), confirming their seniority or accountability level. A different level cadre would not have an overall purview of the organisation and could not have been able to answer a number of questions in the questionnaire.



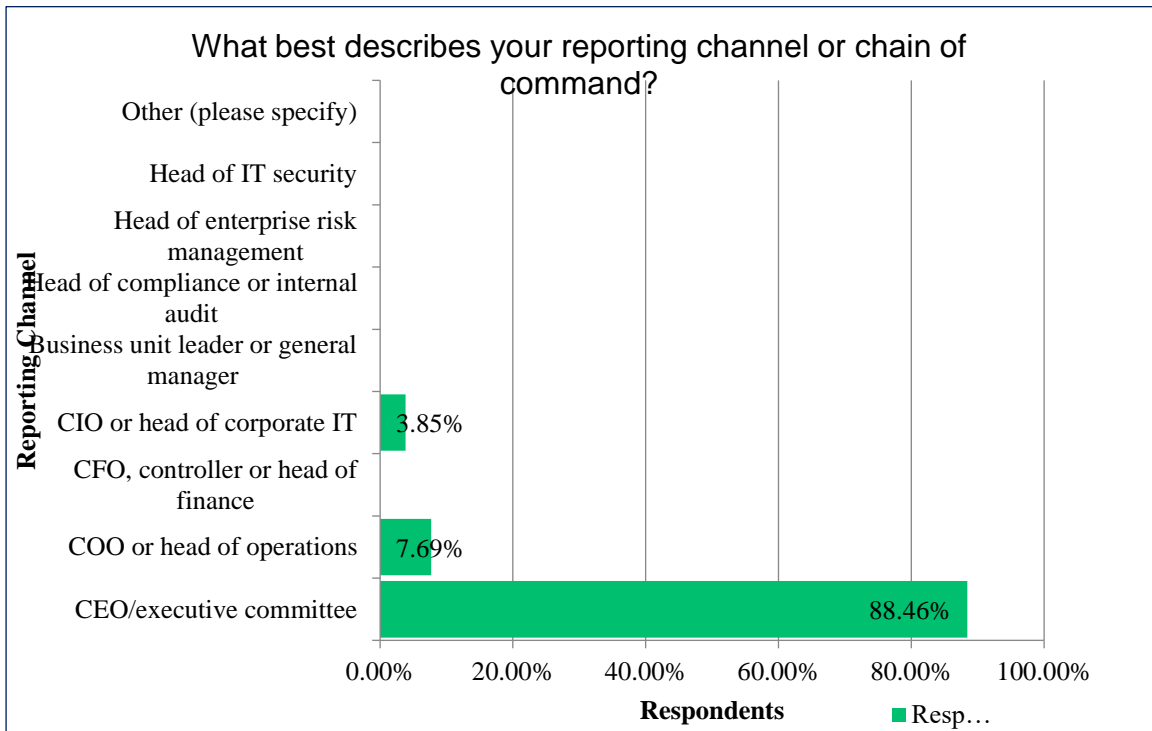
**Figure 4-3: Demographic of respondents by Role focus**

**Table 4-2b: Demographic of respondents by Activities done as part of Role**

<b>Answer Choices</b>	<b>Responses</b>	
Managing budgets	96.15%	25
Evaluating vendors	100.00%	26
Setting priorities	100.00%	26
Securing systems	100.00%	26
Ensuring compliance	96.15%	25
Ensuring system availability	96.15%	25
None of the above	23.08%	6



**Figure 4-4: Demographic of respondents by Position level.**



**Figure 4-5: Demographic of respondents by reporting channel.**

**Staffing capacity**

Concerning staff capacity in the banks, 69% of the participating banks indicated that they have a total staff head count of above one thousand according to results from Figure 4-6. Drilling down further in Figure 4-7, the result shows that majority of the



respondent banks (50%, n=13) indicated that out of the full head count, they have between 5 and 10 dedicated cybersecurity staff. Those with five or more dedicated cybersecurity staff were 18, representing 69% of the respondents.

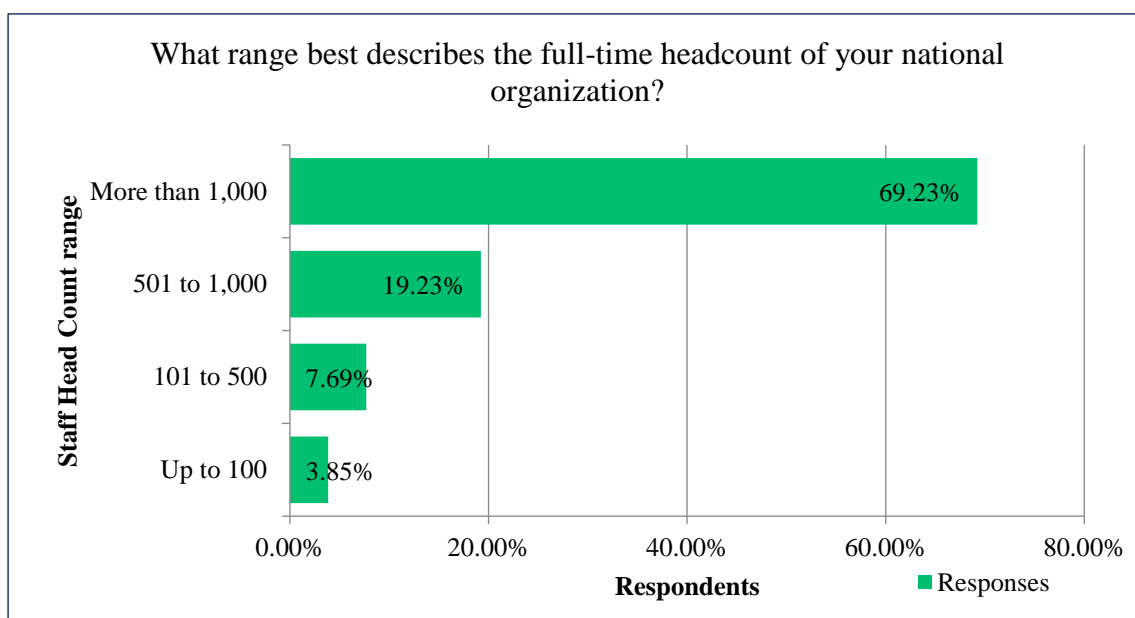


Figure 4-6: Staff head count of respondent banks

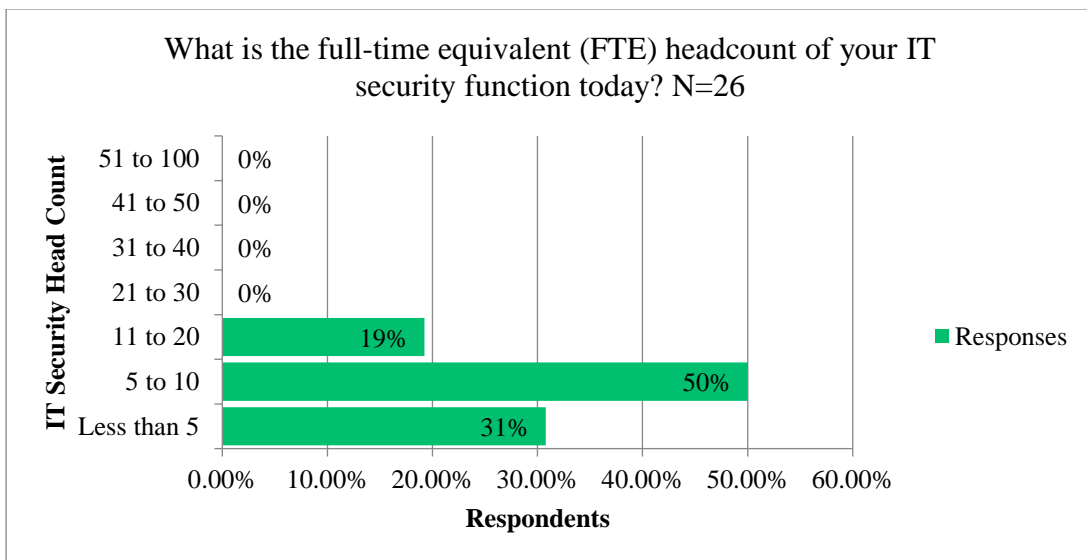
### Capacity to achieve cyber-resilience

Are banks' cyber-security departments understaffed or overstaffed? To answer this question, we correlated current IT security staff count with target full-time IT security head count necessary to achieve cyber-resilience (data as shown in Figure 4-8). The result is as follows.

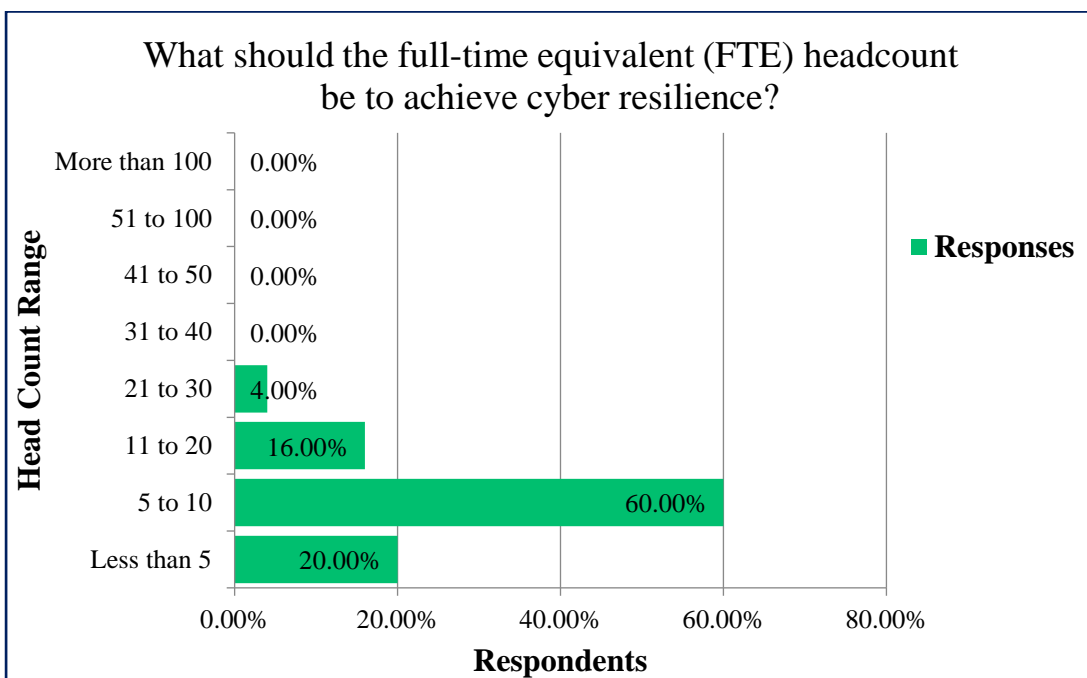
**Table 4-3: Descriptive Statistics for comparing full-time head count in IT department vs desired head count for achieving cyber-resilience.**

Descriptive Statistics			
	Mean	Std. Deviation	N
What is the full-time equivalent (FTE) headcount of your IT security function today?	1.88	.711	26
What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?	1.96	.824	26

Results in table 4-3 indicate that the two questions elicited a response mean tending towards response choice two (Head count 5 to 10) with standard deviation of close to 1 (SD=.71 and .82), indicating that responses varied widely. From the mean, it is clear that the banks indicated to retain the current level of staff count or increase to this level, i.e. Head count 5 to 10, perhaps upgrading from the lower range. The graph in figure 4-7 and figure 4-8 show this relationship.



**Figure 4-7: Full-time head-count of IT cybersecurity team at the bank.**



**Figure 4-8: Full-time headcount required to achieve cyber-resilience.**

Applying Pearson's correlation on the two variables as depicted in table 4-4 indicates a weak positive correlation of .33 whose 2-tailed significance is 0.096, which is greater than the research's chosen significant level of 0.05. This therefore indicates that the two values have no statistical significance. Clearly, the responses were by chance.

**Table 4-4: Correlation of Current IT head count vs required capacity to cyber-resilience**

		What is the full-time equivalent (FTE) headcount of your IT security function today?	What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?
What is the full-time equivalent (FTE) headcount of your IT security function today?	Pearson Correlation	1	.333
	Sig. (2-tailed)		.096
	Sum of Squares and Cross-products	12.654	4.885
	Covariance	.506	.195
What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?	Pearson Correlation	.333	1
	Sig. (2-tailed)	.096	
	Sum of Squares and Cross-products	4.885	16.962
	Covariance	.195	.678

#### 4.3.2 Responses per variable for measuring cyber-resilience

All the variable questions used in cyber-resilience framework and their responses have been provided in Appendix D (Table D-1). For each question used in the instrument to measure cyber-resilience, weighted mean, standard deviation, minimum and maximum values have been provided. The mean values are score-ranked into a scale from 1 (Weak) to 5 (Very Strong), as defined in Table 3-2.

### **4.3.3 Analysis by Objectives**

In this section, the findings of the study have been elaborated based on the objectives, and in a manner that also seeks to answer the underpinning research questions.

### **4.3.4 Identify and defining variables for measuring cyber-resilience**

The first objective of the research was to identify relevant variables or indicators for measuring cyber-resilience. The eight constructs for measuring cyber-resilience were derived from previous research works and frameworks. Seven of the eight constructs were adopted from works by Ponemon Institute (2017, 2018, 2019) that has used the same indicators for three consecutive years, thus providing strong grounds for reliability. The Ponemon indicators are all mutually inclusive with other frameworks and standards reviewed in study. Most frameworks including Ponemon, tend to abide by NIST standard frameworks (Kott and Linkov (2019). Additional amendments were effected especially on the specific questions per construct. The eight constructs were operationalized into the conceptual framework as independent variables, while the cyber-resilience enhancement was operationalized as the effect of the changing individual measures for the eight constructs (dependent variables).

The eight constructs formed the basis for grouping of the individual questions. Each response and constructs were rank-graded into a further 5-level Likert scale rankings as shown in table 3-2 of Chapter 3.

The research sought to measure cyber-resilience of each bank. By applying the foregoing grading scheme per bank, and categorizing these per construct, the outcome is a grading of each respondent's cyber-resilience strength as shown in table 4-7. Note that the names of the respondents have not been used as confidentiality assurance demanded by the banks before accepting to participate in this research.

### **4.3.5 Analysis by constructs**

#### **Perception of the importance of the 8 cyber-resilience constructs**

Respondents were first to rank order eight factors that have been found to be key to achieving a high level of cyber resilience, and which form the basis of this research constructs. The ranking of 1 = most important to 7 = least important was translated into

1-5 Likert grading representing the 5-levels of cyber-resilience strength. Table 4-5 shows the descriptive statistics based on the eight independent variable constructs and the one dependent variable construct.

**Table 4-5: Perception to cyber-resilience constructs**

	Weighted Mean	Std. Deviation	N
1. Preparedness	4.09	.21	26
2. Planned Redundancies	3.61	.41	26
3. Knowledgeable or Expert Staff	4.32	.20	26
4. Governance, Leadership & Compliance	3.72	.12	26
5. Asset Classification & Risk Profiling	4.05	.16	26
6. Ample Resources	2.66	.25	26
7. Agility	2.73	.18	26
8. Strong Security Posture	2.73	.10	26
<b>9. Perception to Cyber-resilience</b>	<b>4.76</b>	<b>.25</b>	<b>26</b>

The findings indicate that the banks' self-assessment perception to cyber-resilience and the value they attached to it is at the highest levels in all areas. From Table 4-5, the independent variable construct Preparedness scored a weighted mean of 4.06, extrapolating to a perception ranking of 5 (Very Strong). Planned Redundancies scored 3.61 (Strong). The odd perception were on Ample Resources and Strong Security Posture. Banks perceptions seem to suggest that Ample Resources and Agility (at M=2.66 and M=2.73 respectively) are only moderately essential for cyber-resilience.

The mean weighted score for Perception to cyber-resilience strength is 4.76 (N=26), extrapolating to an overall ranking of 5 (Very Strong) on this perception.

The conclusion to be drawn from Table 4-5 is that whereas banks see themselves inwardly as very strong (M=4.76, SD=0.25, N=26) in cyber-resilience, however, the public perception is skeptical, going by what is reported in the media (Sunday, 2019;

Muthoni, Karanja & Sunday, 2019). Clearly, there is overconcentration of efforts in Preparedness, business continuity tasks like Planned Redundancies, training staff on skills and awareness, Governance, compliance and asset risk profiling management at the expense of in-depth defence (strong security posture), agility and adaptability, and provision of enough resources. All constructs had a standard deviation of less than 1, indicating that most respondents had less variations in opinions to the indicated outcome.

Pearson's correlation model was used to determine the level and significance of the relationships between each of the eight independent constructs and the dependent construct. The correlation test was computed using a 5% significance level (2-tailed). A two-tailed test was used because the null hypotheses for this research are non-directional. Table 4.6 shows the bi-variate inter-correlation matrix between the construct variables.

**Table 4-6: Correlation matrix between Cyber-resilience variables**

		9.	1.	2.	3.	4.	5.	6.	7.	8.
<b>9. Perception to Cyber-resilience</b>	<i>Pearson's r</i>	1	.203	.498**	.622**	.476*	.455*	.587**	.420*	.366
	<i>Sig. (2-tailed)</i>		.320	.010	.001	.014	.019	.002	.033	.066
<b>1. Preparedness</b>	<i>Pearson's r</i>	.203	1	.305	.079	.123	.160	.214	-.161	.297
	<i>Sig. (2-tailed)</i>	.320		.129	.701	.550	.434	.294	.432	.140
<b>2. Planned Redundancies</b>	<i>Pearson's r</i>	.498**	.305	1	.518**	.670**	.563**	.447*	.036	.296
	<i>Sig. (2-tailed)</i>	.010	.129		.007	.000	.003	.022	.862	.142
<b>3. Knowledgeable/ Expert Staff</b>	<i>Pearson's r</i>	.622**	.079	.518**	1	.590**	.570**	.621**	.185	.324
	<i>Sig. (2-tailed)</i>	.001	.701	.007		.002	.002	.001	.365	.106
<b>4. Governance &amp; Compliance</b>	<i>Pearson's r</i>	.476*	.123	.670**	.590**	1	.447*	.393*	-.090	.389*
	<i>Sig. (2-tailed)</i>	.014	.550	.000	.002		.022	.047	.663	.049
<b>5. Asset Class. &amp; Risk Profiling</b>	<i>Pearson's r</i>	.455*	.160	.563**	.570**	.447*	1	.514**	.045	.335
	<i>Sig. (2-tailed)</i>	.019	.434	.003	.002	.022		.007	.828	.094
<b>6. Ample Resources</b>	<i>Pearson's r</i>	.587**	.214	.447*	.621**	.393*	.514**	1	.383	.269
	<i>Sig. (2-tailed)</i>	.002	.294	.022	.001	.047	.007		.053	.184
<b>7. Agility</b>	<i>Pearson's r</i>	.420*	-.161	.036	.185	-.090	.045	.383	1	.210
	<i>Sig. (2-tailed)</i>	.033	.432	.862	.365	.663	.828	.053		.304
<b>8. Strong Security Posture</b>	<i>Pearson's r</i>	.366	.297	.296	.324	.389*	.335	.269	.210	1
	<i>Sig. (2-tailed)</i>	.066	.140	.142	.106	.049	.094	.184	.304	

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

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

Pearson's r – Pearson's coefficient correlation

Despite being a two-tailed test, at a glance, table 4.6 indicates that majority of the constructs have positive correlation except for three variables: Agility construct which



has a negative but weak correlation with Preparedness (-1.61), and Governance, leadership and compliance (-0.09). This is elaborated further in regression graphs (as shown in Figure 4.9(a) (b)) in which the regression model line passes through quite few plots hence this is an imperfect model.

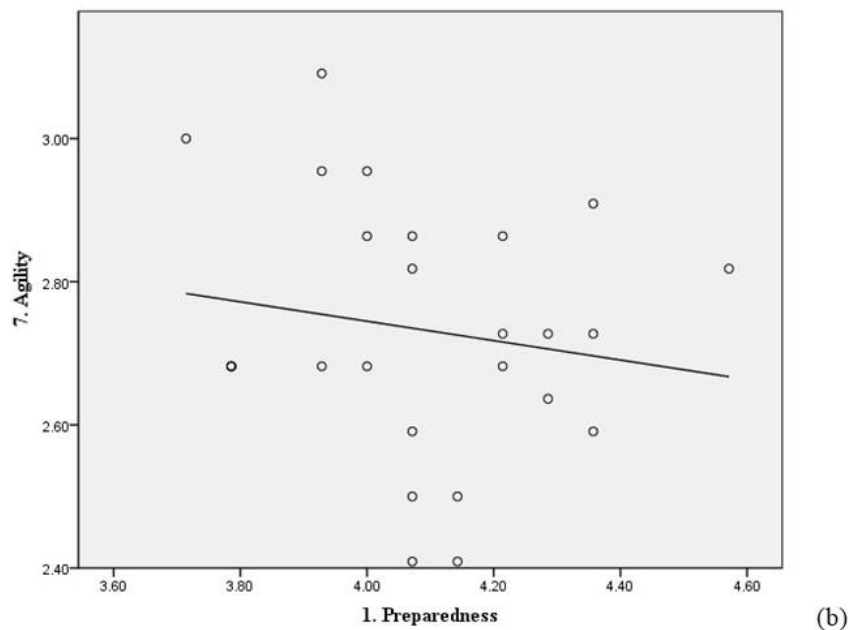
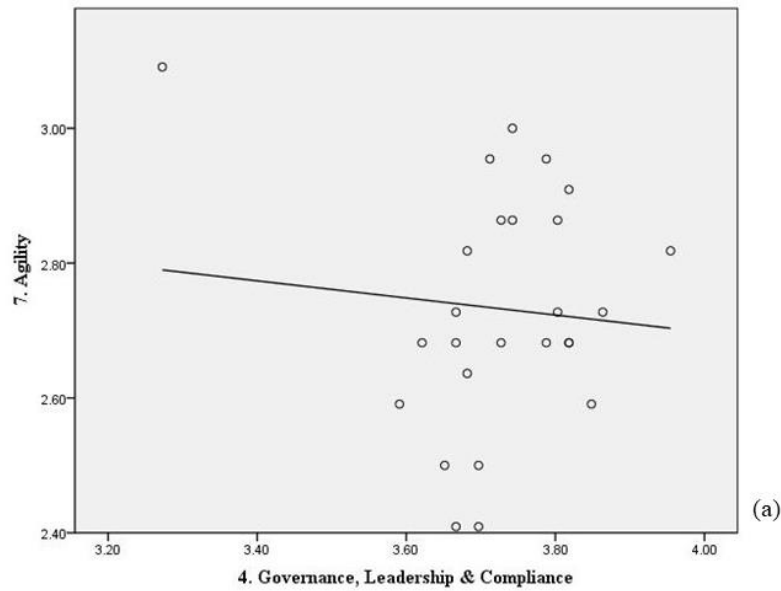


Figure 4-9: Scatter and regression graph for correlation between (a) Agility and Governance, leadership and Compliance, and (b) Agility and Preparedness.

The result suggests that as stronger governance, leadership and compliance factors are implemented in the banks, the agility of the IT department in ensuring cyber-resilience decreases marginally.

### **1. Preparedness**

This construct dealt with a number of factors that influence the responsiveness of a banking institution to cyber-attacks. The banks must have capabilities to respond to cyber incident emergencies in an effective manner (Miora, Kabay & Cowens, 2014, p56.2). Many institutions have adopted operation model of a cybersecurity incident and response team (CSIRT). This is because as digitisation areas increase, the attack surface and intensity of attacks also increase (Ormond & Turnbull, p.172).

#### **Measuring Preparedness**

To measure this construct, a number of questions were fielded to the respondents and were used to rank the bank's preparedness.

#### **Ranking of Preparedness as an important factor for achieving cyber-resilience**

The respondents were first asked to indicate their perception to the importance of Preparedness as a contributing factor to cyber-resilience. On a scale of 1 (most important) to 7 (least important), respondents were meant to rate how important Preparedness is to their quest for cyber-resilience. The overall mean polled 1.85 translating to "Important". The indicators measured a number variables including: existence of a cyber-security incident response plan (CSIRP), CSIRP review frequency, time to awareness of a cybersecurity incident, response time rating, CSIRP resource capacity, and internal incident communication procedure and protocol.

This is broken down further into the contingent factors as shown in Table 4-7.

**Table 4-7: In the past 12 months, how has the time to detect, contain and respond to a cyber-crime incident changed?**

		Significantly increased	Increased	No Increase	Decreased	Significantly Decreased
In the past 12 months, how has the volume of cybersecurity incidents changed?	%	4	46	8	38	4
	<i>f</i>	1	12	2	10	1
In the past 12 months, how has the severity of security incidents changed	%	19	62	8	8	4
	<i>f</i>	5	16	2	2	1
In the past 12 months, how has the time to detect, contain and respond to a cyber-crime incident changed?	%	2	11	0	11	2
	<i>f</i>	8	42	0	42	8
		Very frequently	Frequently	Somewhat frequently	Rarely	Never
As a result of data breaches and cyber-crime incidents, how frequently do disruptions to business processes or IT services occur?	%	0	8	15	73	4
	<i>f</i>	0	2	4	19	1

The analysis shows a perfect balanced split for the time it takes to detect and respond to incidents (Table 4-7). 50% of the respondents indicated that the time has increased while 50% indicated that the time has decreased. Similarly, 50% of the banks indicated that the number of cyber security incidents increased, while another 81% showed that the attacks increased in severity.

#### **Does the bank have a CSIRP in place?**

The research sought to know whether respondent bank has a Cyber Security Incidence and Response Plan (CSIRP), and if it is active. The response data is shown in table 4-8a. Additionally, Figure 4-8b shows the frequency of reviewing CSIRP. The aim of this is understand if banks are well prepared against cyber-attacks.

**Table 4-8:Existence of cyber-security incident response plan (CSIRP**

(a)			(b)		
<i>Does the bank have a CSIRP Plan?</i>			<i>Frequency of reviewing CSIRP?</i>		
	<i>%</i>	<i>f</i>		<i>%</i>	<i>f</i>
We have a CSIRP that is applied consistently across the entire enterprise	88.46	23	Each month	3.85	1
We have a CSIRP, but is not applied consistently across the enterprise	11.54	3	Each quarter	84.62	22
Our CSIRP is informal or “ad hoc”	0.00	0	Biannual	3.85	1
We don’t have a CSIRP	0.00	0	No set time	3.85	1
			Never reviewed	3.85	1

The findings indicates that many banks are prepared and have set up cyber-security incident response plan (CSIRP). 88.46% (N=23) have an active CSIRP while 11.54% (N=3) have an informal CSIRP which is executed at will. Furthermore, over 84.6% of banks that have a CSIRP normally would review it quarterly (N=22).

Why is CSIRP important for a bank? According to Ponemon’s 2018 cyber-resilience research, high performing banks on cyber-resilience were more likely to have a CSIRP in place (Ponemon, 2019).

## 2. Planned Redundancies

Planned redundancies are the main drivers of business continuity and business resilience. Deploying mechanism such as hot-standby, failover redundancy, fail-safe - all are intended to reduce time to recovery.

In this research, bank respondents were asked to rate the importance of the Planned redundancies to their organisations. The weighted mean rating stood at 1.85, extrapolated as “Important” (which stand for a strong “Strong” rating on the cyber-resilience scale).

A number of questions were fielded to measure this construct. The result is shown in tables 4-9, 4-10 and 4-11.

**Table 4-9: How often do you review DR Plan?**

Answer Choices	Responses	
	%	<i>f</i>
Each month	3.85	1
Each quarter	88.46	23
Twice per year	3.85	1
Once each year	0.00	0
No set time period for reviewing and updating the plan	3.85	1
We have not reviewed or updated since the plan was put in place	0.00	0

**Table 4-10: Service level recoverability to customers**

<b>How do you rate your cyber-resiliency with regards to your Service level recoverability requirements to your customers in case of a disruption?</b>		
Answer Choices	Responses	
	%	<i>f</i>
Continuous availability 99.999 percent Zero planned outages	3.85	1
Nearly continuous 99.99 percent Up to four-hour planned outages (maintenance)	19.23	5
High availability 99.9 percent Up to four-hour planned outages (maintenance)	23.08	6
Moderate availability 99.5 percent	53.85	14

**Table 4-11: Rating for cyber-resiliency with regards to Service level**

Answer Choices	Responses	
	%	<i>f</i>
Return to service in less than five minutes (all events)	3.85	1
Local operations: return to service in less than five minutes; Data centre: return to service in less than two hours	11.54	3
Return to service in less than two hours (all events)	73.08	19
Local operations: return to service in less than eight hours; Data centre: return to service in less than specified time frame (days to weeks)	11.54	3

The data indicates that, like CSIRP, many banks take disaster recovery serious and would review it every quarter. Clearly, there is a correlation between the CSIRP and Disaster recovery, both being reviewed every quarterly by 84.62% (N=22) and 88.46 (N=23) respectively. Respondents who selected quarterly review of CSIRP also selected quarterly review of Disaster recovery.

In terms of service continuity and recovery from disaster, only one bank (3.85%) from the respondents is offering the highest level of service availability and business objective assurance. Majority of banks (53.85%, N=14) are providing moderate availability of 99.5%, while 73% (N=19) are willing to provide a service level objective of Return to service in less than two hours for all business events. This, in a digitised economy, is damaging. For a banking institution, it is a reputation problem.

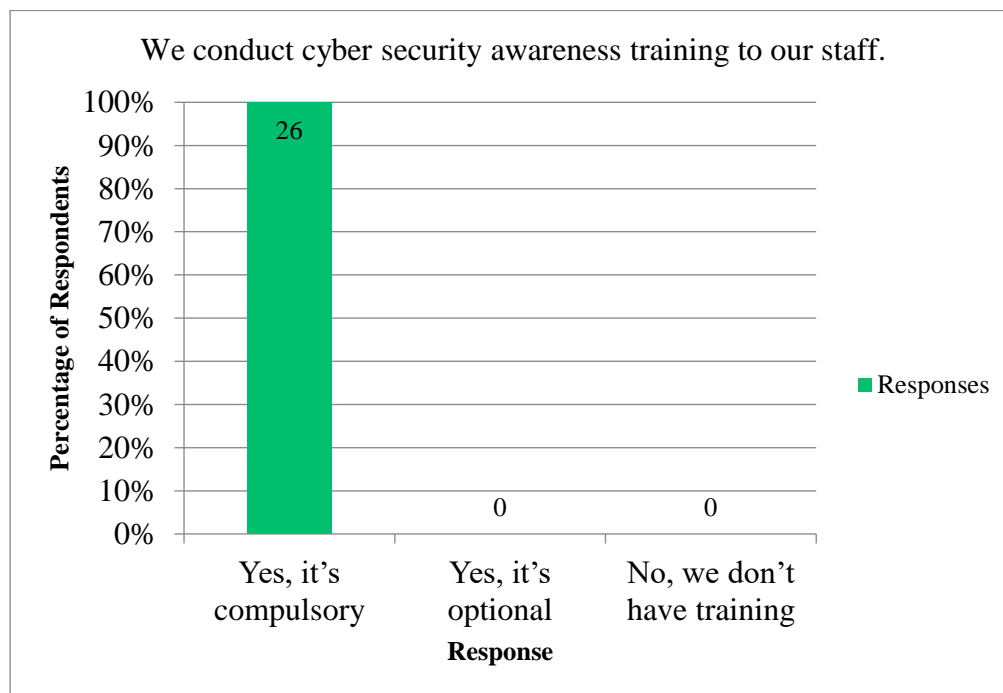
### **3. Knowledgeable/Expert Staff**

The purpose of this construct was to measure the different factors and strategies used by banks to ensure that they have the right mix of staff for cyber security tasks.

By perception, the analysis shows that this was the most well acknowledged constructs, at a weighted mean rating of 1.96. This is a clear indication that there is great emphasis on staff and situation awareness training, nurturing essential skills for cyber-resilience.

Nineteen out of twenty-six (73.08%) respondents indicated that they are very strong in cybersecurity awareness among staff, while 26.92% indicated that they are strong in cybersecurity awareness. Combined, this gives a 100% rating of all banks surveyed to have strong to very strong cybersecurity-aware staff. To this level, all banks (100%, N=26) indicated that they manage and conduct in-house cyber security tests on vulnerability, security audit, penetration testing and vulnerability testing. However, this is only possible if the bank has the right mix of personnel – which is informed by the strong rating of the construct.

Figure 4-10 (a) and (b) indicates a graph depicting respondent banks that conduct cyber security awareness and other training to staff.



**Figure 4-10: (a) Respondent banks that conduct cybersecurity awareness to staff.**



**Figure 4-10: (b) Actions taken by respondent banks to train staff.**

From figure 4-10(a) and (b) above, the research findings indicate that all respondent banks (N=26, 100%) not only conduct cybersecurity awareness training, they have also made the training mandatory.

#### **4. Governance, leadership and compliance**

In this research Governance, leadership and compliance is intended to measure existence of leadership structure, and governance rules such as policies, procedures that govern various aspects of cyber-security and cyber-resilience. The construct goes further to gauge how well a bank is prepared to comply to various regulatory, laws and standards.

Overall, by perception, respondents rate this construct as an Important (Strong) factor for cyber-resilience, at a weighted mean of 1.72. On a cyber-resilience ranking scale, this translates to a Weak score. However, a number of factors hinder this construct. According to the surveyed population, 61.1% (N=11) indicated that insufficient budget supports hinder implementation of proper governance and leadership structure that promote cyber-resilience.

Regarding leadership, 34.6% (N=9) of the surveyed banks have hired a head of cyber-security (Chief Information Security Officer – CISO) specifically charged with

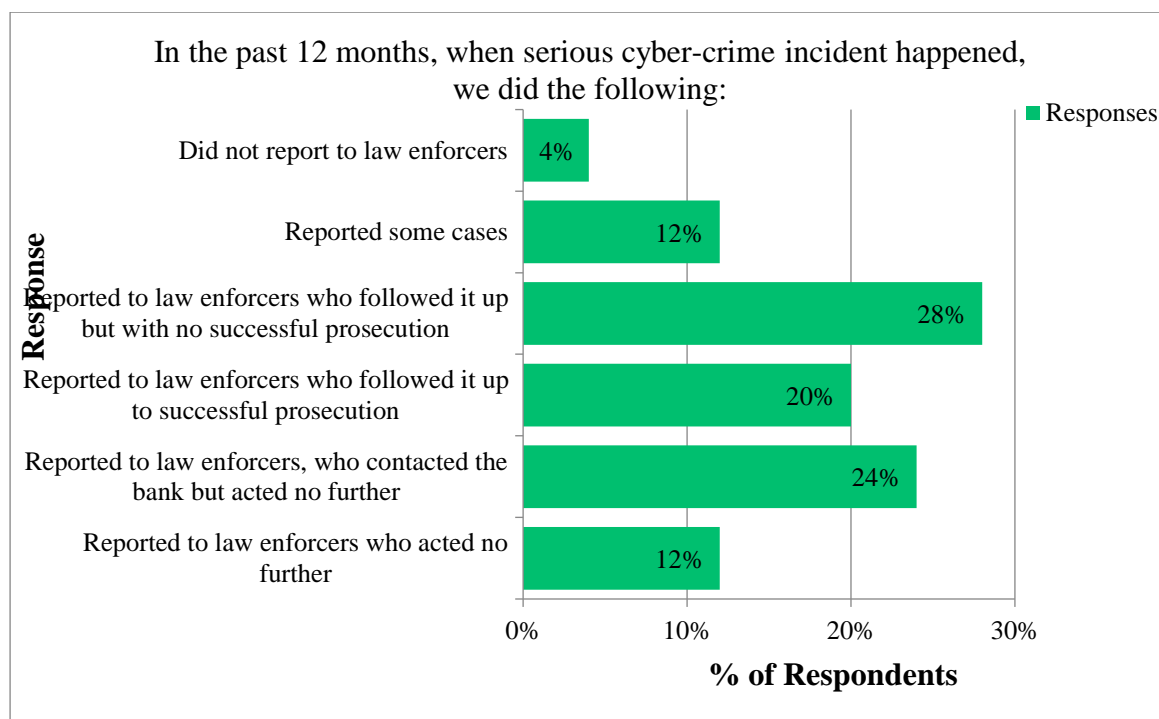


managing all aspects of cyber-security. However, 65.39% (N=17) still have reporting lines to the CIO/CTO. None of the respondents indicated reporting to the CEO. No governance and leadership structure fits all organisations (Harkins, 2016, p.34). The research also sought to know if the banks have established compliance departments. Compliance deals with validating adherence to policies, standards and regulations. The finding is that 65.38% (N=17) of the surveyed banks said that they have internal compliance departments, while 34.62% (N=9) have internal compliance departments supplemented by outsourced compliance services. That gives 100% (N=26) of the respondents having a compliance department.

Serianu (2017) reported that 72% of institutions affected by cybercrime did not report to the authorities. Driven by this perceptions, the research sought to understand if, first, banks were participating in incident sharing, and, second, cyber incidents were being reported to the police. The results are shown in Table 4-12 and Figure 4-11 below:

**Table 4-12: Participation in initiatives for information-sharing**

Does this bank participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?		
Answer Choices	Responses	
	%	<i>f</i>
Yes	96.15	25
No	3.85	1



**Figure 4-11 : Handling of cyber-incidents by law enforcers**

The findings on table 4-12 and figure 4-11 indicate that 96% of the banks (N=25) report all incidents to the police, with exception of 4% (N=1), possibly an outlier result. Majority of the banks (88.46%, N=23) report the cases because it is required by law (see table 4-13).

**Table 4-13: Reasons why a bank would share information about breaches**

Answer Choices	Responses	
	%	<i>f</i>
Improves the security posture of my organization	76.92	20
Improves the effectiveness of our incident response plan	19.23	5
Enhances the timeliness of incident response	15.38	4
Reduces the cost of detecting and preventing data breaches	30.77	8
Fosters collaboration among peers and industry groups	69.23	18
Legal requirements	88.46	23
Not Applicable - We do not share.	0.00	0

Notwithstanding the sharing of incidents, the findings settles the public perception that banks hide cyber incident attacks to protect their reputation.

### **5. Asset Classification and Risk profiling**

Asset Classification and Risk profiling plays a major role in ensuring cyber-resilience. It is the cornerstone of risk-focussed cybersecurity. On the whole, banks ranked this factor as one of the most important factors. On a scale of 1 (most important) to 7 (least important), the weighted mean was 1.77 indicating a strong “Important” rating.

To this end, the research sought to understand what drives the bank to invest in information (cyber) security. The result is shown in Table 4-14 below.

**Table 4-14: What drives the bank to invest in information security (Scale 1-5)**

	Very weak(1)		Weak (2)		Moderate (3)		Strong (4)		Very Strong (5)		Weighted Average
	%	f	%	f	%	f	%	f	%	f	
Protection of information and data	0.0	0	0.0	0	0.0	0	3.9	1	96.2	25	4.96
Prevention of system outages/ business process functionality	0.0	0	0.0	0	0.0	0	3.9	1	96.2	25	4.96
Compliance with authority security requirements	0.0	0	0.0	0	0.0	0	3.9	1	96.2	25	4.96
Safeguard for reputation/ brand image	0.0	0	0.0	0	0.0	0	3.9	1	96.2	25	4.96
Support for bank's business goals	0.0	0	0.0	0	0.0	0	15.4	4	84.6	22	4.85
Compliance with security requirements imposed by clients	0.0	0	0.0	0	0.0	0	38.5	10	61.5	16	4.62
Enabler for digital transformation	0.0	0	0.0	0	0.0	0	7.7	2	92.3	24	4.92
Safeguard of humans	0.0	0	0.0	0	0.0	0	26.9	7	73.1	19	4.73
Increase of efficiency/cost reduction	0.0	0	0.0	0	3.85	1	3.9	1	92.3	24	4.88

From Table 4-14, it can be inferred most respondents surveyed concentrated their responses on level 5 (Very Strong). None of the respondents was below level 4 (Strong).

## 6. Ample Resources

Ample resources returned a strong response from the surveyed banks. On a scale of 1 (most important) to 7 (least important), the mean weighted response was 1.81

indicating that availability of ample resources is an ingredient to building stronger cyber-resilience.

The construct sought to understand human resource capacity and the bank's perception to its adequacy and budget allocations. We performed a one-tailed correlation to understand the relationship directions of the key indicators for human resource capacity. The findings are shown on Table 4-15.

Full-time headcount (FHE) of the whole bank staff has a positive correlation coefficient of .528 with Full-time-equivalent (FTE) headcount of IT security staff, with significance of .003. Compared with the research's level of significance (p-value) of .005, the findings indicate that this correlation is statistically significant confirming that the total number of staff in the organisation significant affect the number of hires for IT security department. However, against the Targeted IT security headcount, it shows that most banks surveyed were arbitrary in their numbers. At a significance of .09 (more than the p-value significance of .05) and the correlation coefficient of .272, this is a weak correlation, hence the conclusion that these values were by chance.

**Table 4-15: Pearson correlation- Staff head counts**

		The full-time headcount of your national organization	full-time equivalent (FTE) headcount of your IT security function	Target full-time equivalent (FTE) headcount for cyber resilience
The full-time headcount of your national organization.	Pearson Correlation	1	.528**	.272
	Sig. (1-tailed)		.003	.090
full-time equivalent (FTE) headcount of your IT security function	Pearson Correlation	.528**	1	.333*
	Sig. (1-tailed)	.003		.048
Target full-time equivalent (FTE) headcount for cyber resilience	Pearson Correlation	.272	.333*	1
	Sig. (1-tailed)	.090	.048	

\*. Correlation is significant at the 0.05 level (1-tailed).

As there is no standard rule for staff capacity for achieving cyber-resilience per organisation, the result appear to suggest that the arbitrary staffing shows that each bank implements its own staffing capacity.

Taken from another angle by comparing the same variables against budget, it can be inferred from Table 4-16 below, that there are very low coefficient factors (.316 and .091), and significant values are more than p-value of .05 (.058 and .329). Conclusively, the budget values are arbitrary and by chance and have no relationship with staffing capacity. In this circumstance, it is possible that budget figures indicated by the respondents could have included other elements other than just cyber-security.

**Table 4-16: Pearson Correlation of IT security headcount vs targeted headcount**

		Cyber security budget	full-time equivalent (FTE) headcount of your IT security function	Target full-time equivalent (FTE) headcount for cyber resilience
	Pearson Correlation	1	.316	.091
Cyber security budget	Sig. (1-tailed)		.058	.329
full-time equivalent (FTE) headcount of your IT security function	Pearson Correlation	.316	.316	.091
	Sig. (1-tailed)	.058		.048
Target full-time equivalent (FTE) headcount be to achieve cyber resilience	Pearson Correlation	.091	.333*	1
	Sig. (1-tailed)	.329	.048	

\*. Correlation is significant at the 0.05 level (1-tailed).

## 7. Agility

Agility as defined by Worley et al. (2014), is the ability for banks to make timely, effective and sustained response to a changing circumstance. A number of indicators were formulated to measure this construct.

On a scale of 1 (most important) to 7 (least important), respondents were asked to rate how important Agility is to their quest for cyber-resilience. Even though the overall weighted mean of the responses rated 1.85 (equivalent to “Important”), the breakdown on the responses that influence Agility exposed the problematic area. The result is shown in Table 4-17.

**Table 4-17: Assessing factors that influence Agility**

	1		2		3		4		5		Mean
	Very Low 1 or 2		Low 3 or 4		Moderate 5 or 6		High 7 or 8		Very High 9 or 10		
	%	<i>f</i>	%	<i>f</i>	%	<i>f</i>	%	<i>f</i>	%	<i>f</i>	
The bank’s ability to prevent a cyber-attack.	0.0	0	0.0	0	0.0	0	46.2	12	53.9	14	4.5
The ability to quickly detect a cyber-attack	0.0	0	0.0	0	0.0	0	50.0	13	50.0	13	4.5
The bank’s ability to contain a cyber-attack.	0.0	0	0.0	0	0.0	0	50.0	13	50.0	13	4.5
How valuable cyber-resilience is to the Bank.	0.0	0	0.0	0	0.0	0	34.5	9	65.4	17	4.7
The importance of having skilled cybersecurity professionals in your (CSIRP).	0.0	0	0.0	0	0.0	0	38.5	10	61.5	16	4.6
How difficult it is for the bank to hire and retain skilled IT security personnel	42.3	11	15.4	4	0.0	0	19.2	5	23.1	6	2.7
Weighted average 1.85 ( extrapolated as Important)											

The findings indicate that banks are having a problem hiring skilled IT security personnel who can champion cybersecurity and cyber-resilience. This is not a new problem; it transcends Kenyan borders. Serianu (2017) highlights the skills shortage in

cybersecurity in Kenya as one of the greatest contributor to vulnerabilities. A similar question in Ponemon's research in 2018 (Ponemon, 2019) indicates that the problem improved marginally in 2018 (75% of respondents) over 2017 research (77% of respondents). This could explain why Agility was one of the two worst performing constructs, second to Security Posture.

## **8. Strong Security Posture**

As has been noted, as a construct variable, Strong Security Posture had the lowest rating of all constructs. The importance of Strong Security Posture was indicated by surveyed banks as "Important" underpinning its significance in cyber-resilience.

Analysing Security Posture required fielding numerous questions to the respondents covering many aspects of cybersecurity such as in-depth security implementations, advancement in tools, cybersecurity maturity, number of reported incidents and those thwarted – basically, a measure of success rates in preventing incidents and ensuring availability of business operations. The ultimate goal of Strong Security is to ensure the three core principles of security are ensure: availability, integrity and confidentiality.

### **Cybersecurity Maturity level**

Respondents were asked to indicate their cybersecurity maturity based on a four-stage model defined by Ponemon (Ponemon, 2018c). At the infant stages, there is Early stage. At this stage, many cybersecurity program activities have not yet been planned or deployed; at Middle stage, cybersecurity program activities are planned and defined but only partially deployed; at Late-middle stage, many cybersecurity program activities are deployed across the enterprise, finally, Mature stage. At this stage, core cybersecurity program activities are deployed, maintained and/or refined across the enterprise. The response data is summarised in table 4-18.



**Table 4-18: What best describes the maturity level of the bank's cybersecurity program or activities?**

Answer Choices	Responses	
	%	<i>f</i>
<b>Early stage</b> – many cybersecurity program activities have not as yet been planned or deployed	0.00%	0
<b>Middle stage</b> – cybersecurity program activities are planned and defined but only partially deployed	23.08%	6
<b>Late-middle stage</b> – many cybersecurity program activities are deployed across the enterprise	46.15%	12
<b>Mature stage</b> – Core cybersecurity program activities are deployed, maintained and/or refined across the enterprise	30.77%	8

The findings indicate that out of all the banks surveyed, only eight banks (30.77%) have attained a full maturity stage status. The modal maturity stage is Late-middle representing 12 banks (46.15%).

When correlated with cyber security budget per bank, the findings indicate that the correlation factor is positive at .536, significant at .002. With Significant value less than p-value .005, the correlation value is significant, suggesting that there is a strong positive relationship. Hence, it is appropriate to infer that higher budget for cyber security contributed to maturity factors. Hence, bigger banks with disposable budget have a higher chance to accelerate cyber security maturity level and hence, cyber-resilience.

#### **4.4 Test of Hypotheses Analysis of Variance**

The structural conceptual model consisted of nine null hypotheses. Regression model and analysis of variance (ANOVA) were used as tools to test the relationship between variables and to understand the effects the independent variables have on dependent variables. Specifically, ANOVA was used to test for hypothesis as defined

in section 3.12.3. The summary of the hypothesis test results are shown in table 4-19 below:

- Assumptions for the tests were: Alpha  $\alpha$  Significance level of .05;
- degree of freedom  $df(1,24)$
- Decision:
  - If F-Value > F-critical - reject null Hypothesis;
  - If F-Value < F-critical - accept null hypothesis
  - For Hypothesis  $H_{01}$  –
    - Reject
      - If  $N > 13$ ; weighted mean  $\geq 3$
    - Accept
      - If  $N > 13$ ; weighted mean  $< 3$

**Table 4-19: Summary of Status of Hypothesis testing**

Null Hypotheses	$R^2$	p-value	F-value	F-critical	Decision F-Value > F-critical	Null Hypothesis Status
<b><math>H_{O_1}</math></b> : Majority of banks in Kenya are not cyber-resilient	<b>All banks (N=26) (Strong)</b>		<b>weighted mean &gt; 3</b>			<b>Rejected</b>
<b><math>H_{O_2}</math></b> : Agility factors do not have an effect on cyber-resilience enhancement perceptions in banks.	<b>.177</b>	<b>.03</b>	<b>5.15</b>	<b>4.26</b>	<b>True</b>	<b>Rejected</b>
<b><math>H_{O_3}</math></b> : Preparedness factors do not have an effect on cyber-resilience enhancement perceptions in banks.	<b>0.41</b>	<b>.32</b>	<b>1.03</b>	<b>4.26</b>	<b>False</b>	<b>Accepted</b>
<b><math>H_{O_4}</math></b> : Strong security posture has no bearing on cyber-resilience enhancement perceptions in banks.	<b>.13</b>	<b>.07</b>	<b>3.72</b>	<b>4.26</b>	<b>False</b>	<b>Accepted</b>
<b><math>H_{O_5}</math></b> : Redundancy planning has no effect on cyber-resilience enhancement perceptions in banks.	<b>.25</b>	<b>.01</b>	<b>7.92</b>	<b>4.26</b>	<b>True</b>	<b>Rejected</b>
<b><math>H_{O_6}</math></b> : Knowledgeable and expert staff have no effect on cyber-resilience enhancement perceptions in banks.	<b>.39</b>	<b>.00</b>	<b>15.17</b>	<b>4.26</b>	<b>True</b>	<b>Rejected</b>
<b><math>H_{O_7}</math></b> : Ample resources do not have effect on cyber-resilience enhancement perceptions in banks.	<b>.35</b>	<b>.00</b>	<b>12.64</b>	<b>4.26</b>	<b>True</b>	<b>Rejected</b>
<b><math>H_{O_8}</math></b> : Governance, leadership and compliance factors have no	<b>.23</b>	<b>.01</b>	<b>7.04</b>	<b>4.26</b>	<b>True</b>	<b>Rejected</b>

Null Hypotheses	$R^2$	p-value	F-value	F-critical	Decision F-Value > F-critical	Null Hypothesis Status
effect on cyber-resilience enhancement perceptions in banks.						
Classification and risk profiling of assets have no bearing on cyber-resilience enhancement perceptions in banks	.21	.02	6.28	4.26	True	Rejected

SPSS was used to fit the simple linear regression model over all dependent and independent variables together as group, the output is a model summary (Table 4-20), an ANOVA analysis (Table 4-21) and a coefficients table (Table 4-22). From Table 4-20, the value of  $R^2$  (.59) predicts the variance accounted for by the predictor variables included in the model. As to whether this contribution is statistically significant, we compared the p-value (sig=.027) from ANOVA table (Table 4-22) with alpha value (.05). Since  $p < .05$ , it means that the values of the model are significant.

In conclusion, the overall regression model shown is significant,  $F(8,17)=3.00$ ,  $p=.027$ ,  $R^2=.59$ . It also indicates that this regression analysis is statistically significant in that when all the predictors are taken together as a group, they predict Cyber-resilience perception significantly.

**Table 4-20: Model Summary – all variables together**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.765 <sup>a</sup>	.585	.390	.19777

*a. Predictors: (Constant), 8. Strong Security Posture, 7. Agility, 2. Planned Redundancies, 1. Preparedness, 3. Knowledgeable or Expert Staff, 5. Asset Classification & Risk Profiling, 6. Ample Resources, 4. Governance, Leadership & Compliance*

**Table 4-21: ANOVA<sup>a</sup>– all variables together**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.939	8	.117	3.001	.027 <sup>b</sup>
	Residual	.665	17	.039		
	Total	1.604	25			

*a. Dependent Variable: 9. Perception to Cyber-resilience*

*b. Predictors: (Constant), 8. Strong Security Posture, 7. Agility, 2. Planned Redundancies, 1. Preparedness, 3. Knowledgeable or Expert Staff, 5. Asset Classification & Risk Profiling, 6. Ample Resources, 4. Governance, Leadership & Compliance*

**Table 4-22: Coefficients<sup>a</sup>– all variables together**

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-1.582	2.219		-.713	.486
	1. Preparedness	.205	.227	.169	.900	.381
	2. Planned Redundancies	.039	.150	.064	.261	.798
	3. Knowledgeable/Expert Staff	.368	.302	.291	1.220	.239
	4. Governance, Leadership & Compliance	.434	.517	.214	.840	.413
	5. Asset Classification & Risk Profiling	.126	.351	.078	.359	.724
	6. Ample Resources	.076	.241	.074	.314	.758
	7. Agility	.546	.286	.380	1.907	.074
	8. Strong Security Posture	-.016	.487	-.006	-.032	.974

*a. Dependent Variable: 9. Perception to Cyber-resilience*

#### 4.4.1 Test of Hypotheses per predictor variables

There are nine null hypotheses to test as part of this research (see table 4-19).

##### **Test of Hypothesis two**

Null Hypothesis $H_{O_2}$	<i>Agility factors do not have an effect on cyber-resilience enhancement perceptions in banks</i>
Alternate Hypothesis $H_{A_2}$	<i>Agility factors have an effect on cyber-resilience enhancement perceptions in banks</i>

By generating a linear regression model of the Agility predictor variable against dependent variable (Cyber-resilience perception), table 4-23 shows the output of the model summary. The output shows an  $R^2=.177$ .

**Table 4-23 Model Summary for Agility**

Model	R	R-Square	Adjusted R-Square	Std. Error of the Estimate
1	.420 <sup>a</sup>	0.177	0.142	0.235

a. Predictors: (Constant), 7. Agility

The  $R^2$  value indicates that 17.7% of the variance in Cyber-resilience perception can be attributed to or be explained uniquely by Agility factors. As to whether this is a significant contribution, can be explained further by the ANOVA results on Table 4-24. Using alpha value=.05, degree of freedom  $df(1,24)$  to derive f-critical value =4.26 from the F-distribution table.

**Test:** F-value (5.15) is greater than f-critical(4.26).

**Decision:** The null hypothesis is, rejected.

**Conclusion:** The findings therefore indicate that the variance in Cyber-resilience perception can be attributed to or be explained by Agility factors.

**Table 4-24 Analysis of variance (ANOVA<sup>a</sup>) for Agility perceptions on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.283	1	.283	5.151	.033 <sup>b</sup>
	Residual	1.321	24	.055		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 7. Agility

**Test of Hypothesis three**

Null Hypothesis $H_0_3$	<i>Preparedness factors do not have an effect on cyber-resilience enhancement perceptions in banks</i>
Alternate Hypothesis $H_A_3$	<i>Preparedness factors have an effect on cyber-resilience enhancement perceptions in banks.</i>

Table 4-25 shows the output of the linear regression model summary for Preparedness. The output shows  $R^2=.041$ .

**Table 4-25 Model Summary for Preparedness**

Model	R	R Square	Adjusted Square	Std. Error of the Estimate
1	.203 <sup>a</sup>	.041	.001	.25313

a. Predictors: (Constant), 1. Preparedness

The significance of the  $R^2$  is confirmed by an F-test. Taking alpha significance level (.05), degree of freedom  $df(1,24)$  from table 4-27, F-value (1.03) to derive critical f-value from F-Distribution tables as 4.26.

**Test:** F-value (1.03) < F-critical value (4.26).

**Decision:** Null hypothesis is accepted.

**Conclusion:** The analysis leads to acceptance of the null hypothesis  $H_{O_3}$ , and the conclusion that Preparedness factors did not have an effect on respondents cyber-resilience enhancement perceptions in banks.

**Table 4-26 Coefficients<sup>a</sup> for Preparedness perceptions on cyber-resilience**

		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
Model	(Constant)	.760	.990		3.799	.001
1	1. Preparedness	.246	.242	.203	1.017	.320

a. Dependent Variable: 9. Perception to Cyber-resilience

**Table 4-27 Analysis of variance (ANOVA<sup>a</sup>) for Preparedness perceptions on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.066	1	.066	1.033	.320 <sup>b</sup>
	Residual	1.538	24	.064		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 1. Preparedness



### **Test of Hypothesis Four**

---

Null Hypothesis  $H_0_4$       *Strong security posture has no bearing on cyber-resilience enhancement perceptions in banks*

---

Alternate Hypothesis  $H_A_4$     : *Strong security posture has bearing on cyber-resilience enhancement perceptions in banks.*

---

The linear regression model summary for the Strong Security Posture predictor variable against dependent variable (Cyber-resilience perception) is shown in table 4-28. The output shows the coefficient of determination  $R^2$  value = .13.

**Table 4-28 Model Summary for Strong Security Posture**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.366 <sup>a</sup>	.134	.098	.24055

a. Predictors: (Constant), 8. Strong Security Posture

---

Using an F-test to confirm the significance of the  $R^2$ , we take alpha significance level as (.05), degree of freedom  $df(1,24)$  from table 4-29, F-value (3.72) from table 4-29 to derive critical f-value from F-Distribution tables as 4.26.

**Test:** F-value (3.72) < F-critical value (4.26).

**Decision:** Null hypothesis is Accepted.

**Conclusion:** Consequently, even though the value of  $R^2$  (.13) shows that 13% of the variance in Cyber-resilience perception can be explained by factors implemented in Strong Security Posture, that contribution is too insignificant to be used to accept the null hypothesis, judging from the perspective of the respondents.

**Table 4-29 Analysis of variance (ANOVA<sup>a</sup>) for Strong Security posture perceptions on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.215	1	.215	3.718	.066 <sup>b</sup>
	Residual	1.389	24	.058		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 8. Strong Security Posture

**Table 4-30 Coefficients<sup>a</sup> for Strong Security posture perceptions on cyber-resilience**

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.244	1.308		1.716	.099
	8. Strong Security posture	.924	.479	.366	1.928	.066

a. Dependent Variable: 9. Perception to Cyber-resilience

### **Test of Hypothesis Five**

Null Hypothesis $H_0_5$	<i>Redundancy planning has no effect on cyber-resilience enhancement perceptions in banks</i>
Alternate Hypothesis $H_A_5$	<i>Redundancy planning has effect on cyber-resilience enhancement perceptions in banks.</i>

Table 4-31 shows the summary of the computed regression model. The regression model has been used to predict the Cyber-resilience perception based on variations in Redundancy Planning factors. The model has a coefficient of determination  $R^2 = .25$  (from table 4-31), suggesting that the proportion of variance in Cyber-resilience perception explained by Redundancy Planning as a factor of cyber-resilience is 25%.

**Table 4-31 Model Summary for Redundancy Planning**

Model	R	R Square	Adjusted Square	R	Std. Error of the Estimate
1	.498 <sup>a</sup>	.248	.217		.22415

a. Predictors: (Constant), 2. Planned Redundancies

Using an F-test to confirm the significance of the  $R^2$ , we take alpha significance level as (.05), degree of freedom  $df(1,24)$  from table 4-32, F-value (7.92) from table 4-32 to derive critical f-value from F-Distribution tables as 4.26.

**Test:** F-value (7.92) > F-critical value (4.26).

**Decision:** Null hypothesis is Rejected.

**Conclusion:** The findings indicate that 25% of cyber-resilience can be explained Redundancy Planning factors. The research findings lead to the conclusion that respondents perception of the effects of Redundancy Planning on cyber-resilience were significant enough to warrant rejection of the null hypothesis.

**Table 4-32 Analysis of variance (ANOVA<sup>a</sup>) for Redundancy Planning effects on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.398	1	.398	7.924	.010 <sup>b</sup>
	Residual	1.206	24	.050		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 2. Planned Redundancies

**Table 4-33 Coefficients<sup>a</sup> for Redundancy Planning effects on cyber-resilience**

		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
Mode	(Constant)	.664	.394		9.310	.000
1	8. Strong Security posture	.305	.108	.498	2.815	.010

a. Dependent Variable: 9. Perception to Cyber-resilience

### **Test of Hypothesis Six**

---

Null Hypothesis  $H_0$ : *Knowledgeable and expert staff have no effect on cyber-resilience enhancement perceptions in banks.*

---

Alternate Hypothesis  $H_A$ : *Knowledgeable and expert staff have effect on cyber-resilience enhancement perceptions in banks.*

---

The linear regression model summary for the Knowledgeable or expert staff predictor variable against dependent variable (Cyber-resilience perception), is shown in table 4-34. The output shows the coefficient of determination  $R^2$  value = .39.

**Table 4-34 Model Summary for Knowledgeable or Expert Staff**

Model	R	R Square	Adjusted Square	R	Std. Error of the Estimate
1	.622 <sup>a</sup>	.387	.362		.20235

a. Predictors: (Constant), 3. Knowledgeable or Expert Staff

Using an F-test to confirm the significance of the  $R^2$  value, we take alpha significance level as (.05), degree of freedom  $df(1,24)$  from table 4-35, F-value (15.17) from table 5-32 to derive critical f-value from F-Distribution tables as 4.26.

**Test:** F-value (15.17) > F-critical value (4.26).

**Decision:** Null hypothesis is Rejected.

**Conclusion:** The findings indicate that contribution by Knowledgeable/Expert staff as effects on cyber-resilience was significant at the  $R^2$  value of .39. The findings of this test lead to the conclusion that respondents perception of the effects of promoting Staff awareness and Expertise on cyber-security factors were significant enough to warrant rejection of the null hypothesis.

**Table 4-35 Analysis of variance (ANOVAa) for Knowledgeable or Expert Staff effects on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.621	1	.621	15.174	.001 <sup>b</sup>
	Residual	.983	24	.041		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 3. Knowledgeable or Expert Staff

**Table 4-36 Coefficients<sup>a</sup> for Knowledgeable or Expert Staff on cyber-resilience**

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.360	.875		1.555	.133
	3 Knowledgeable or Expert Staff	.787	.202	.622	3.895	.001

a. Dependent Variable: 9. Perception to Cyber-resilience

### **Test of Hypothesis Seven**

---

Null Hypothesis  $H_0$ : *Ample resources do not have effect on cyber-resilience enhancement perceptions in banks*

---

Alternate Hypothesis  $H_A$ : *Ample resources factors affect cyber-resilience enhancement perceptions in banks.*

---

A linear regression model for summary for Ample Resources predictor variable against dependent variable (Cyber-resilience perception) was produced using SPSS as shown in table 4-37. Also, ANOVA results are also provided on table 4-38.

Table 4-37 indicates a computed  $R^2$  of .35. To test whether this is significant, an F-test is performed, using alpha significance level as (.05), degree of freedom  $df(1,24)$  from table 4-38, F-value (12.64) from table 4-38 to derive critical f-value from F-Distribution tables as 4.26.

**Test:** F-value (12.64) > F-critical value (4.26).

**Decision:** Null hypothesis is Rejected.

**Conclusion:** The findings indicate that 35% of cyber-resilience perceptions can be explained by Ample Resources. The findings of this test lead to the conclusion that there is strong significance that factors of Ample Resources for cyber-security have an effect on cyber-resilience perception.

**Table 4-37 Model Summary for Ample resources**

Model	R	R Square	Adjusted Square	R	Std. Error of the Estimate
1	.587 <sup>a</sup>	.345	.318		.20923

a. Predictors: (Constant), 6. Ample Resources

---

**Table 4-38 Analysis of variance (ANOVA<sup>a</sup>) for Ample resources effects on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.553	1	.553	12.638	.002 <sup>b</sup>
	Residual	1.051	24	.044		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 6. Ample resources

**Table 4-39 Coefficients<sup>a</sup> for Ample resources on cyber-resilience**

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.163	.452		.992	.000
	6. Ample resources	.602	.169	.587	.555	.002

a. Dependent Variable: 9. Perception to Cyber-resilience



### **Test of Hypothesis Eight**

---

Null Hypothesis  $H_0$ : *Governance, leadership and compliance factors have no effect on cyber-resilience enhancement perceptions in banks.*

---

Alternate Hypothesis  $H_A$ : *Governance, leadership and compliance factors affect cyber-resilience enhancement perceptions in banks.*

---

Table 4-40 shows the summary of the computed simple linear regression model. The regression model has been used to predict the Cyber-resilience perception based on variations in factors of Governance, leadership and compliance. The model has computed a coefficient of determination  $R^2 = .23$  (from table 4-40), indicating that the proportion of variance in Cyber-resilience perception explained by Governance, leadership and compliance as factors of cyber-resilience is 23%.

**Table 4-40 Model Summary for Governance, Leadership & Compliance**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.476 <sup>a</sup>	.227	.195	.22731

---

a. Predictors: (Constant), 4. Governance, Leadership & Compliance

---

Acceptance of this  $R^2$  value is pegged on its significance. To test whether this is significant, an F-test is performed, using alpha significance level as (.05), degree of freedom  $df(1,24)$  from table 4-41, F-value (7.04) from table 4-41 to derive critical f-value from F-Distribution tables as 4.26.

**Test:** F-value (7.04) > F-critical value (4.26).

**Decision:** Null hypothesis is Rejected.

**Conclusion:** The findings indicate that 23% of cyber-resilience perceptions can be explained by Governance, leadership and compliance effects. The research concludes

that respondents perception of the effects of Governance, leadership and compliance on cyber-security and cyber-resilience was significant enough to warrant rejection of the null hypothesis. Thus, it can be deduced that banks strongly agreed that Governance, leadership and compliance factors affect cyber-resilience enhancement perceptions in banks.

**Table 4-41 Analysis of variance (ANOVA<sup>a</sup>) for effects of Governance, Leadership and Compliance on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.364	1	.364	7.042	.014 <sup>b</sup>
	Residual	1.240	24	.052		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 4. Governance, Leadership & Compliance

### **Test of Hypothesis Nine**

Null Hypothesis **HO<sub>9</sub>**: *Classification and risk profiling of assets have no bearing on cyber-resilience enhancement perceptions in banks*

Alternate Hypothesis **HA<sub>9</sub>**: *Classification and risk profiling of assets have bearing on cyber-resilience enhancement perceptions in banks.*

Simple linear regression has been used to show the behavior of cyber-resilience perception reacts when factors for Asset classification and risk profiling are applied. Table 4-43 shows an output summary of the linear regression model done using SPSS. The table shows that the variance in Cyber-resilience perception is explained by an  $R^2$  value of .21 (from table 4-43) equivalent to 21%.

An F-test is performed to confirm significant of the  $R^2$  and to test for hypothesis. Using alpha significance level as (.05), degree of freedom  $df(1,24)$  from table 4-44, F-value (7.04) from table 4-44 to derive critical f-value from standard F-distribution tables as 4.26.

**Test:** F-value (6.283) > F-critical value (4.26).

**Decision:** Null hypothesis is Rejected.

**Conclusion:** The findings indicate that 21% of cyber-resilience perceptions is attributed to by effects of Asset Classification and risk profiling. The research concludes that this contribution by Asset Classification and risk profiling was significant enough to warrant rejection of the null hypothesis.

**Table 4-43 Model Summary for Asset Classification & Risk Profiling**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.455 <sup>a</sup>	.207	.174	.23014

a. Predictors: (Constant), 5. Asset Classification & Risk Profiling

**Table 4-44 Analysis of variance (ANOVA<sup>a</sup>) for effects of Asset Classification & Risk Profiling on cyber-resilience**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.333	1	.333	6.283	.019 <sup>b</sup>
	Residual	1.271	24	.053		
	Total	1.604	25			

a. Dependent Variable: 9. Perception to Cyber-resilience

b. Predictors: (Constant), 5. Asset Classification & Risk Profiling

### **Test of Hypothesis One**

---

Null Hypothesis  $H_0_1$ : *Majority of banks in Kenya are not cyber-resilient*

---

Alternate Hypothesis  $H_A_1$ : *Majority of banks in Kenya are cyber-resilient.*

---

In validating this hypothesis, the research based its facts on the outcome of the survey, relied on to provide concrete validation whether banks in Kenya are cyber-resilient or not. From raw responses, weighted mean were computed and rank-scored according to a defined scale in table 3-2.

At the lowest level, respondent have been ranked according to weighted mean based on their response characteristics. Full data is shown in Appendix C (table C-3). The data in table D-1 has been analysed per respondent by their research code to provide the ranking below. The result of the individual respondent ranking is shown in table 4-46 below.

**Table 4-46: Cyber-resilience weighted mean and strength grade score**

Position	Respondent Code	Weighted Mean	Grade Score	Position	Respondent Code	Weighted Mean	Graded Score
1	BNK024	3.88	4	14	BNK025	3.57	4
2	BNK018	3.83	4	15	BNK007	3.56	4
3	BNK032	3.74	4	16	BNK028	3.56	4
4	BNK040	3.71	4	17	BNK026	3.55	4
5	BNK037	3.69	4	18	BNK039	3.55	4
6	BNK022	3.68	4	19	BNK023	3.53	4
7	BNK019	3.66	4	20	BNK002	3.50	4
8	BNK013	3.65	4	21	BNK016	3.50	4

---

9	BNK027	3.65	4	22	BNK034	3.50	4
10	BNK012	3.63	4	23	BNK010	3.48	4
11	BNK021	3.63	4	24	BNK035	3.41	4
12	BNK030	3.62	4	25	BNK005	3.39	4
13	BNK003	3.60	4	26	BNK020	3.23	4

The result reveals that all the respondent banks (100%, N=26) yielded weighted means greater than 3 (minimum mean =3.23, maximum =3.88), the level for a Strong cyber-resilience strength, as per the grading scale on table 3-2. It is fair to submit that all the banks surveyed exhibited a Strong cyber-resilience strength. The listing also serves as the ranking of cyber-resilience in which BNK024 can be inferred as the best performer, scoring 3.88 (Strong).

#### **Cyber-resilience respondent rating per constructs**

The result above is elaborated further in the respondents breakdown per construct in Table 4-47. For each respondent, the weighted mean score and the Graded Strength score are by each construct is shown per respondent.

The result shows that BNK24 attained best weighted mean for Strong Security posture (M=2.98, “Moderate”), Agility was led by BNK12 (M=3.17, “Strong”), Governance, leadership and compliance (BNK040, M=3.90, “Strong”).

**Table 4-47: Grading of Respondent cyber-strength per construct (n=26)**

		Cyber-resilience measurement constructs								
		Strong Security Posture 8	Agility 7	Ample Resources 6	Asset Classification & Risk Profiling 5	Governance, Leadership & Compliance 4	Knowledgeable or Expert Staff 3	Planned Redundancies 2	Preparedness 1	
RESPONDENT RESEARCH CODE		Mean Grade	Mean Grade	Mean Grade	Mean Grade	Mean Grade	Mean Grade	Mean Grade	Mean Grade	Overall Weighted Mean
<b>1</b>	<b>BNK002</b>	2.73	2.67	3.00	4.00	3.74	4.29	3.50	4.07	<b>3.50</b>
<b>2</b>	<b>BNK003</b>	2.84	3.13	3.25	4.17	3.75	4.43	3.25	4.00	<b>3.60</b>
<b>3</b>	<b>BNK005</b>	2.73	2.58	2.88	3.94	3.71	3.86	3.25	4.14	<b>3.39</b>
<b>4</b>	<b>BNK007</b>	2.80	2.83	3.00	4.17	3.85	4.29	3.75	3.79	<b>3.56</b>
<b>5</b>	<b>BNK010</b>	2.55	2.58	3.13	4.00	3.74	4.29	3.50	4.07	<b>3.48</b>
<b>6</b>	<b>BNK012</b>	2.64	3.17	3.38	4.17	3.78	4.43	3.75	3.71	<b>3.63</b>
<b>7</b>	<b>BNK013</b>	2.75	3.04	3.25	4.17	3.76	4.43	3.75	4.07	<b>3.65</b>
<b>8</b>	<b>BNK016</b>	2.67	2.83	3.13	4.06	3.82	4.43	3.25	3.79	<b>3.50</b>
<b>9</b>	<b>BNK018</b>	2.89	3.00	3.50	4.28	3.72	4.43	4.25	4.57	<b>3.83</b>
<b>10</b>	<b>BNK019</b>	2.84	2.71	3.13	4.17	3.88	4.43	3.75	4.36	<b>3.66</b>
<b>11</b>	<b>BNK020</b>	2.71	3.13	2.88	3.72	3.29	3.71	2.50	3.93	<b>3.23</b>
<b>12</b>	<b>BNK021</b>	2.67	2.79	3.50	4.17	3.72	4.43	3.50	4.29	<b>3.63</b>
<b>13</b>	<b>BNK022</b>	2.85	3.04	3.50	4.17	3.78	4.43	3.50	4.21	<b>3.68</b>
<b>14</b>	<b>BNK023</b>	2.67	2.83	3.50	4.11	3.66	4.43	3.25	3.79	<b>3.53</b>
<b>15</b>	<b>BNK024</b>	2.98	3.00	3.50	4.33	3.99	4.43	4.75	4.07	<b>3.88</b>
<b>16</b>	<b>BNK025</b>	2.67	2.75	2.88	4.17	3.63	4.43	4.00	4.07	<b>3.57</b>
<b>17</b>	<b>BNK026</b>	2.80	2.83	3.00	4.00	3.76	4.29	3.50	4.21	<b>3.55</b>
<b>18</b>	<b>BNK027</b>	2.73	3.13	3.38	4.06	3.82	4.43	3.75	3.93	<b>3.65</b>
<b>19</b>	<b>BNK028</b>	2.73	2.88	3.13	3.67	3.84	4.29	3.75	4.21	<b>3.56</b>

<b>20</b>	<b>BNK030</b>	2.79	2.92	3.13	4.17	3.71	4.43	3.50	4.36	<b>3.62</b>
<b>21</b>	<b>BNK032</b>	2.67	3.08	3.38	4.17	3.85	4.43	4.00	4.36	<b>3.74</b>
<b>22</b>	<b>BNK034</b>	2.84	2.83	2.88	4.17	3.71	4.43	3.25	3.93	<b>3.50</b>
<b>23</b>	<b>BNK035</b>	2.54	2.63	2.75	4.17	3.69	3.86	3.50	4.14	<b>3.41</b>
<b>24</b>	<b>BNK037</b>	2.68	3.04	3.38	4.17	3.84	4.43	4.00	4.00	<b>3.69</b>
<b>25</b>	<b>BNK039</b>	2.78	2.83	3.13	4.06	3.85	4.29	3.50	4.00	<b>3.55</b>
<b>26</b>	<b>BNK040</b>	2.89	2.92	3.50	4.22	3.90	4.43	3.50	4.29	<b>3.71</b>
<b>Mean</b>		<b>3.00</b>	<b>3.31</b>	<b>3.69</b>	<b>4.77</b>	<b>4.00</b>	<b>4.88</b>	<b>4.04</b>	<b>4.62</b>	

### Cyber-resilience rating by constructs

At a higher level, weighted means were computed and aggregated per construct, as shown in Table 4-48. Table 4-48 also shows corresponding ranking grade description.

**Table 4-48: Weighted mean of Cyber-strength by constructs**

	Mean	Std. Deviation	N	Ranking grade	Ranking Description
1. Preparedness	4.09	.21	26	5	Very Strong
2. Planned Redundancies	3.61	.41	26	4	Strong
3. Knowledgeable or Expert Staff	4.32	.20	26	5	Very Strong
4. Governance, Leadership & Compliance	3.72	.12	26	4	Strong
5. Asset Classification & Risk Profiling	4.05	.16	26	5	Very Strong
6. Ample Resources	2.66	.25	26	3	Moderate
7. Agility	2.73	.18	26	3	Moderate
8. Strong Security Posture	2.73	.10	26	3	Moderate
9. Perception to Cyber-resilience	4.76	.25	26	5	Very Strong

The result indicates that banks perception to cyber-resilience is Very Strong. The weighted mean for Preparedness is M=4.09 with Standard deviation of .21, Staff training (M=4.32, SD=.20), Asset classification and risk management (M=4.05, SD=.16), Cyber-resilience perception (M=4.76), and on Governance and compliance (M=3.72), and Planned redundancies (M=3.61). The weakest constructs were Agility, Secure Posture and Ample resources each returning a mean of 2.66, 2.73, 2.73 respectively. The standard deviations were below 0.3, suggesting that responses had minimal variation.

Breaking down the above statistics further, the means above are represented by the frequencies in table 4-49 below.

**Table 4-49: Number of banks categorised by Cyber-resilience strength and construct**

Construct	Very				Very
	Weak	Weak	Moderate	Strong	Strong
1. Preparedness				10	16
2. Planned Redundancies			1	23	2
3. Knowledgeable/ Expert Staff				3	23
4. Governance, Leadership & Compliance				26	
5. Asset Classification/Risk Profiling				9	17
6. Ample Resources			26		
7. Agility			25	1	
8. Strong Security Posture			26		
9. Perception to Cyber-resilience					26

#### 4.5 Overall Cyber-resilience score and posture

**Test:** 100% of respondents (N=26) scored weighted mean > 3.0 (from table 4-47)



**Decision:** Weighted mean of 3.0 or more is equivalent to Strong. Over 50% of the banks are Strong in Cyber-resilience. Majority of banks are Strong in Cyber-resilience. Null hypothesis is rejected.

**Conclusion:** From the foregoing results in table 4-46, table 4-47 and table 4-48, and using the sampled respondent banks as representing the entire population of banks, it can be inferred that majority of banks are strongly cyber-resilient. Thus, the hypothesis  $H0_1$  that banks in Kenya are not cyber-resilient has been rejected based on the statistical analysis.

## **CHAPTER FIVE – DISCUSSION, CONCLUSION AND RECOMMENDATIONS**

### **5.1 Introduction**

This section presents discussions and counter-arguments from what the results of the data analysis reveals. Towards the end of the chapter, a summary of the researcher's conclusions are made and recommendations proposed.

While the objective to develop a framework appeared achieved, this chapter also aims to answer the pertinent question from the research: are Kenyan banks cyber-resilient?

### **5.2 Discussions**

At the onset, the research had set out three key research questions to drive the objectives. The discussions that follow flow per research question.

#### **5.2.1. What are the acceptable instruments and indicators necessary for assessing cyber-resilience of Kenyan banks?**

The research has successfully collated developed a localized cyber-resilience measurement tool, derived from prior frameworks and literature review, in order to make it the tool comprehensive. Measure indicators from prior works from NIST, CERT-RMM model, Serianu were combined with Ponemon Institute's Cyber-resilience tool to create a local framework known as Cyber-Resilience For Banks (CRF4Banks). CRF4Banks incorporates indicators specifically suited for Kenyan Banking industry, where certain unique threats exist that are uncommon in developed countries – that of mobile money fraud. The also takes into consideration the legal framework existing in Kenya besides the international regulations and obligations.

#### **5.2.2. To what degrees of measure are Banks in Kenya cyber-resilient?**

Using the developed instrument (CRF4Banks), it was possible to measure cyber-resilience strength of Kenyan banks and to answer this question. One of the null hypothesis was that banks in Kenya are not cyber-resilient. In the survey conducted using the CRF4Banks instrument, the research was able to measure and grade cyber-

resilience of the participating banks based on their perception to eight key cyber-resilience constructs.

From the survey results, all banks in Kenya that participated (N=26) attained weighted mean above 3, which corresponds to grade ranking of “Strong”. This represents 65% of the sampled banks, and 59% of all the banks in Kenya. It can be concluded that this is representative enough to generalize that banks in Kenya exhibit “Strong” cyber-resilience posture.

A number of indicators contributed to this. Staff education and awareness were mentioned factors that contributed to strong cyber-resilience. Other constructs that indicate strong areas of focus by banks are Preparedness (weighted mean of 4.09) which ensures business continuity and business resilience; Asset classification and risk management (weighted mean=4.05).

### **5.2.3. How many banks in Kenya are prepared if and when a cyberattack takes place?**

It has been acknowledged that cyber-attacks are inevitable events, even with the most expensive security options. Cyber-resilience attempts to provide an assurance of continuity during such moments. From this survey outcome, 100% (N=26) of the respondents banks ranked a strong cyber-resilience in all the eight constructs. Therefore, all the banks, were found to be resilient to cyber-attacks.

### **5.2.4. Do banks hide vulnerabilities and losses?**

A public perception at the onset of the research indicated that banks may not be truthful with information on risks from cyber attacks (Olingo,2018; Ombati, 2017). From the research findings, 96% of the surveyed banks reported suspected cyber crime to the authorities, for which they left legal processes to take control. However, it emerged from the study that the authorities only managed to pursue and conclude 20% of the case. It is unclear why this is so, but could be explained by other factors outside the purview of this research. It is therefore conclusive to state that banks have been prudent by reporting cases to law enforcers.

### **5.2.5. Discussions on Constructs for measuring cyber-resilience**

From the research findings, respondents indicated that they placed high value on Preparedness, Planned Redundancies, Knowledgeable or Expert staff, Governance, leaders and compliance, Asset classification and risk profiling as factors important for achieving cyber-resilience. Average perceptions were however recorded for Ample Resources, Agility and Strong Security Posture.

After correlating the constructs, the research found that some of the variables had an impact on effectiveness of one another. For example, results showed that stronger governance, leadership and compliance factors cause a marginal decrease in Agility of the IT department in ensuring cyber-resilience. This could explain that stronger governance and compliance, (such as strong supervision on policies, regulations, compliance and cyber-resilience leadership hierarchy) had a negative bearing on cyber-resilience. It could also suggest that unwarranted bureaucracies were slowing down reaction or response time, and hence affecting other variables such as Preparedness and Strong Security Posture.

#### **Preparedness**

All the surveyed banks (10=Strong, 16=Very Strong) indicated strong levels of Preparedness, with most (N=23) reporting having a CSIRP reviewed mostly (85% of the banks) quarterly. From the results, it appears that there is a unanimity of quarterly review of a CSIRP in Kenyan banks even though there is no internationally agreed frequency. However, it is essential that this is done as frequently as possible and at closer interval due to fast-changing vulnerability landscape, according to Ponemon (2019). The existence of a CSIRP, however, is a strong indication of a bank that has embraced cyber-resilience, according to Ponemon (2019). Despite this strong rating, many more banks (50%) experienced increased volume of cyber-security incidents, and a further 81% describing the attacks as more severe. The outcome shows that that no matter how strong security principles were implemented, cyber threats will still penetrate. The good news is, 77% of the banks indicated that even though the attacks were more severe, they rarely or never disrupted business, indicating strong resilience. The outcome shows a mix performance when compared to Ponemon's 2018 research

(Ponemon, 2019) in which 26% reported that time had significantly increased, 30% (increased), 31% (unchanged), 9% decreased and 3% (decreased significantly).

### **Knowledgeable and expert staff**

According to findings of the research, all surveyed banks (N=26) conduct mandatory cyber security awareness, while 96% of the banks sponsor specialized training for IT security personal. From the foregoing, there is strong evidence that banks have attached great importance to eliminating the weakest point for vulnerabilities in any organisation, according to NIST.

### **Asset Classification and Risk profiling**

There are a number of factors that drive banks to invest in cyber security. From the research outcome, many organisations have placed emphasis on protecting assets and reducing risk factors. All the factors for Asset Classification and Risk profiling put to the respondents returned weighted means greater than 4 (Very Strong) indicating great emphasis banks have on the factors. Of notable concern was the factor “Safeguard of humans”. The findings in this research suggest that safeguarding human life is only taken as a topmost priority by 73% (N=19) of the respondents. According to NIST Risk Management Framework (RMF) principles, any cybersecurity intervention is considered a failure if life is lost, regardless of how strong or compliant the procedure is, and results in a risk factor of 100% - for example, putting first responders or customers at harms-way in an operation to deal with a cyber-threat.

### **Leadership and Governance**

Most banks take cognizant of the importance of having a dedicated leader to manage cyber-security and manage cyber-resilience. To this effect, may banks (over 42%, n=11) have had and maintained a CISO for between 4 and 6 years, in an environment where skills are few and personnel are difficult to retain.

### **Cyber risk insurance**

The inevitability of cyber-attacks makes insurance of assets against such risk important. The research sought to know what mechanism banks are using to transfer cyber-security risk. Nearly 90% of the banks have not purchased cyber-risk policies.

This is an area that needs further research, in order to understand what hinders the growth.

### **5.3 Summary of main findings**

The key takeaway from this research is that banks in Kenya have made strides in adopting best practices to secure their assets against cyber threats. Resilience in the cyber-space has been a growing concern for many banks. The following summarise the main findings.

1. The research successfully developed a Kenyan-based instrument for assessing cyber-resilience status of banks.
2. Banks in Kenya have a strong cyber-resilience posture. The survey revealed that many banks improved on many indicators spanning 2 years: improved defense mechanisms, increased use of technology in cybersecurity, increased budget, widespread adoption of best practices, increased budget allocation to cyber-security and cyber-resilience, and above all, a major security training awareness for staff.
3. Training of staff on cybersecurity awareness has been a key focus by many banks, perhaps an overconcentration.
4. Majority of banks do not purchase cybersecurity risk transfer (cyber-insurance) as a risk mitigation measure. It is difficult to understand why, considering the inevitability of cyber-attacks.
5. Lack of prosecutorial expertise to handle cyber security cases has made it difficult to follow up and close cyber crime cases. This could be attributed to lack of comprehensive legal framework and digital forensic expertise.
6. Banks experience some level of difficulty in hiring and retaining cybersecurity experts. Literature review and cybersecurity reports show that there is an acute shortage of cybersecurity experts in Kenya and all institutions including banks are pursuing the available few.

### **5.4 Conclusion**

The aim of this study was to develop a framework for measuring cyber-resilience of banks in Kenya, and to use the framework to assess their cyber-resilience posture. A quantitative approach was adopted using a range of complementary statistical methods.

The study has provided insights on the status of cyber-resilience in Kenya banks and the current worldview from literature review. It has also identified a range of metrics and their groupings (constructs) that befitted as key factors that influence and can be used to measure cyber-resilience. Although this was a relatively small-scale study, confidence in the generalisability of the findings is enhanced by the fact that there was a high level of consistency in the findings, culminating into consistently high scores of cyber-resilience among the banks, confirming a notable level of consensus among participating banks.

The eight dominant cyber-resilience constructs that were identified in this research should not be considered discrete but as the cyber-security landscape keeps on evolving. However, they embody key themes that anchor future research on cyber-resilience frameworks. Current discourse in cybersecurity is increasingly advocating for increased focus on cyber-resilience, on realization that cyber-attacks are inevitable eventualities in business enterprises. Since banks share an ecosystem with other organisations, cyber-resilience should be given more focus by all enterprises to ensure cyber-safety at each level.

The conclusions drawn from this research are multifold. First, Kenyan banks are strong in cyber-resilience. Kenya's banking sector has embraced cyber-resilience principles culminating into a strong rating as witnessed in the research. The apparently high level of consistency across the participating banks suggests that the instrument's measurement variables consisted of factors that were generic and relevant to the banks' cyber-resilience. Responses from the research indicate that there is growing awareness and internalization of cyber-resilience in many banks in Kenya and it gradually transforming into a healthy cyberspace environment. However, since the cyberspace is shared, cyber-resilience needs to permeate into other institutions that collaborate with the banking institutions. There is also need to develop an inclusive framework that can provide a fair assessment of cyber-resilience of any institution.

Secondly, developing a framework for measuring cyber-resilience in banks, and indeed in other institutions will still be a challenging task due to the ever-evolving threat landscape, because of faster obsolescence of tools and methods for assessing cybersecurity. For example, a number of indicators included in the instrument measured perceptions on use of current technologies such as artificial intelligence, machine

learning and analytics to boost cybersecurity. The relevance of such indicators may reduce in future.

Furthermore, with multiple threat landscape, the number of measurement indicators may need to expand in order to measure cyber-resilience comprehensively. However, that will become a challenge to research respondents when this is reflected in a lengthy questionnaire.

Finally, having a common cyber-resilience framework is essential in harmonizing cyber-resilience assessment. In view of the remit of this study, it is hoped that the findings will spur more discussion and development in the cyber-resilience domain.

## **5.5 Recommendations**

Cyber-resilience is not a destination. Challenges that hinder strengthening of cyber-resilience will persist as vulnerabilities become more innovative in order to access the prized targets, the banks. Organisations must be ready to adopt the eight tenets of cyber-resilience set out in this research in order to become cyber-resilient. Based on the research findings, a number of recommendations were been derived.

With regard to the first research problem, the lack of a locally harmonised framework for assessing banks was a challenge. This study has revealed that this can be easily solved by wider participation of stakeholders in the banking in the development of a unified cyber-resilience framework, in much the same way that there exists financial prudential guidelines. This can easily be championed by the regulator CBK and the bank's lobby group, Kenya Bankers Association.

There is also need to explore and invest in newer technologies that are more dynamic in managing cyber-resilience, such as automation, machine learning, artificial intelligence and process orchestrations to lessen the effort of threat hunting. Automation reduces the time to identify and contain incidents and augment that threaten cyber-resilience. It also strengthens cybersecurity incident response plan (CSIRP). Second, it enhances threat intelligence with the ability to provide early warnings. Third, there are many metrics for measuring threats, therefore, automation reduces the complexity of managing cybersecurity. A regular review of internal cyber-security and cyber-resilience policies will be healthy way forward.

Banks should also provide incentives to staff to upskill in cybersecurity and resilience. This is because there are less skilled personnel in this area in Kenya. This



will go a long way in alleviating the skill shortage, and deepen discourse on cyber-resilience.

Furthermore, Banks and other organisations need to increase adoption of cyber insurance as a way of transferring the inevitable cyber risks.

The government of Kenya should hasten resolution of the recent Computer Misuse and Crimes 2018 Act, which is currently under a court suspension. This will provide a framework for prosecuting cyber-crime cases, and perhaps increase the prosecution success rates. Furthermore, training of law enforcers on digital forensics and cyber-crime should be increased. It is not clear how many skilled personnel exist in this area in Kenya, but it could be a factor that contributed to the lower success rate in prosecuting cases mentioned in the research findings.

### **5.6 Areas of Further Research**

Cyber-resilience is not a silo effort. As revealed in the research finds, the Mobile money transfer and mobile banking were the most used channels to commit cybercrime. Vulnerabilities created by third-party systems can result into losses in a banking institution. Therefore, in future, cyber-resilience of banks should incorporate financial intermediaries such as mobile money operators, money transfer organisations, and bank agents.

The research did not factor in software development life cycle. There is need to incorporate these into the framework for measuring cyber-resilience.

Respondents complained of lengthy questionnaire. This is true because a complete characterization of cyber-resilience incorporates huge list of variable metrics. There is need to explore options to shorten the instrument's indicators.

Many banks indicated that they do not insure against cybercrime losses. This area requires further study to understand the contributing factors.

## REFERENCES

- Antikainen, J. (2014, December). *Model for national cybersecurity resilience and situation awareness improvement*. Retrieved September 22, 2018, from [https://www.theseus.fi/bitstream/handle/10024/86179/opinnaytetyo\\_%20Jani%20Antikainen.pdf?sequence=3](https://www.theseus.fi/bitstream/handle/10024/86179/opinnaytetyo_%20Jani%20Antikainen.pdf?sequence=3)
- Antonucci, D. (2017). *Cyber Risk Handbook: Creating and measuring effective cybersecurity capabilities*. New Jersey: John Wiley & Sons.
- Asia Bankers Association (2019, June 30). Retrieved July 15, 2019 from <https://www.aba.org.tw/2019/07/30/cyber-resilience-is-the-future-of-cybersecurity/>.
- Attiah, A., Chatterjee, M. and Zou, C. C. (2018). A Game Theoretic Approach to Model Cyber Attack and Defense Strategies. Paper presented at the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO. pp.1-7. doi:10.1109/ICC.2018.8422719.
- BBC. (2016, March 22). Kenya Revenue Authority 'lost \$39m to hacker'. Retrieved from <https://www.bbc.com/news/world-africa-39351172>
- Bell, J. (1987). *Doing your research project*. Philadelphia: Open University Press.
- Bosworth, S., Kabay, M.E. & Whyne, E. (2014). *Computer Security Handbook*. 6th Edition. New Jersey: Wiley.
- Caballero, A. (2009). Information Security essentials for IT Mangers: Protecting Mission-critical systems. In J.R. Vacca (Eds.), *Computer and Information Security Handbook*. USA: Elsevier Inc.
- Caralli, R. A., Allen, J. H., White, D.W., Young, L.R, Mehravari, N. & Curtis, P. D. (2016). *CERT Resilience Management Model, Version 1.2*. Software Engineering Institute. Retrieved 31 Dec, 2018 from [https://resources.sei.cmu.edu/asset\\_files/Handbook/2016\\_002\\_001\\_514462.pdf](https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf)
- Central Bank of Kenya.(2017a). *Bank Supervision: Annual Report*. Retrieved from [https://www.centralbank.go.ke/uploads/banking\\_sector\\_annual\\_reports/1818825039\\_2017%20Annual%20Report.pdf](https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/1818825039_2017%20Annual%20Report.pdf)
- Central Bank of Kenya.(2017b). *Guidance Note on Cybersecurity*. Retrieved from [https://www.centralbank.go.ke/uploads/banking\\_circulars/634077191\\_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf](https://www.centralbank.go.ke/uploads/banking_circulars/634077191_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf)
- Clark, V.L.P. & Creswell, J.W. (2015). *Understanding Research: A Consumer's Guide*. (2nd Ed). New Jersey: Pearson.
- Cochran, W. G. (1963). *Sampling Techniques*. (2nd Ed.). New York: John Wiley and Sons, Inc

- Comfort, L. K., Boin, A., & Demchak, C. C. (2010). *Designing Resilience: Preparing for Extreme Events*. In L. K. Comfort, A. Boin, & C. C. Demchak (Eds.), *Designing Resilience: Preparing for Extreme Events*. Pittsburgh: University of Pittsburgh Press.
- Cooper, D. R. & Schindler, P. S.(2014). *Business Research Methods*. (12th Edition). New York : McGraw-Hill.
- Crown. (2009, June). *Cybersecurity Strategy of the United Kingdom: safety, security and resilience in cyber space*. Retrieved September 22, 2018, from <http://webarchive.nationalarchives.gov.uk/+http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>
- Dalziell, E.P. & McManus, S.T. (2008). Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance. Retrieved from <https://www.researchgate.net/publication/29489371>
- Department of Homeland Security (DHS). *Cybersecurity and Infrastructure Security Agency (CISA): Infrastructure Security*. Retrieved from <https://www.dhs.gov/cisa/overview>
- Dhingra, A., Gryseels, M., Kaplan, J., and Lung, H. (2018). *Digital resilience: Seven practices in cybersecurity*. Retrieved Dec 19, 2018 from <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-blog/digital-resilience-seven-practices-in-cybersecurity>.
- Erbschloe, M. (2017). *Threat Level Red: Cybersecurity Research Programs of the U.S. Government*. USA: CRC Press.
- European Union. (March, 2017). *Cybersecurity in the European Digital Single Market*. Retrieved from [https://scienceofcybersecurity.files.wordpress.com/2017/09/i\\_sam\\_cybersecurity\\_report.pdf](https://scienceofcybersecurity.files.wordpress.com/2017/09/i_sam_cybersecurity_report.pdf)
- European Union. (2019). *Cyber Resilience for Development*. Retrieved July 17, 2019 from <https://cyber4dev.eu/>
- Grant, C. & Osanloo, A. (2014). *Understanding, selecting, and integrating a theoretical framework in dissertation Research Creating the blueprint for your “House* Retrieved from <https://files.eric.ed.gov/fulltext/EJ1058505.pdf>
- Gagliardone, I., & Sambuli, N. (2015). *Cybersecurity and Cyber Resilience in East Africa*. Retrieved from [http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2015/06/Gagliardone\\_Sambuli\\_CyberSecurity-2.pdf](http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2015/06/Gagliardone_Sambuli_CyberSecurity-2.pdf)
- Gay, L.R., Mills, G. E. and Airasian, P.W.(2012). *Educational Research: Competencies for analysis and applications*. (10th Edition). USA:Pearson
- Goodwin, P. and Smith, A. (2018). *The State of IT Resilience*. Retrieved from <https://www.zerto.com/wp-content/uploads/2018/08/State-of-IT-Resilience-2018-IDC.pdf>
- Gordon, L. E. (2016). *Real Research-Research Methods Sociology Students Can Use*. United States: Sage Publications, Inc

- Harkins, M.W. (2016). *Managing Risk and Information Security*. (2<sup>nd</sup> Ed). CA:Apress Open
- IBM. (2011). *The evolution of business resiliency management: A proactive guide to helping you strengthen your business resiliency management program*.
- ITU. (2017). *Global Cybersecurity Index (GCI) 2017*. Retrieved from ITU: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf)
- Kakah, M. (2016, March 26). *Court detains computer geek in Sh4bn KRA case for 40 days*. [Nation Online]. Retrieved 19 December, 2018 from <https://www.nation.co.ke/news/Alex-Mutungi-Mutuku-KRA-cybercrime-kenya/1056-3867562-10bq6hvz/index.html>
- Keys, B. & Shapiro, S. (2019). Frameworks and Best Practices. In A. Kott, & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks*. Switzerland: Springer.
- Kenya Bankers Association (2019). KBA Members. Retrieved 20 February, 2019 from <http://www.kba.co.ke/members.php>
- Kothari, C.R.(2004). *Research Methodology: Methods & Techniques*. (2nd Ed). India: New Age International
- Kott, A. & Linkov, I. (2019). *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. In A. Kott, & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks*. Switzerland: Springer.
- Kumar, R.(2011). *Research Methodology: A step-by-step guide for beginners*. (3rd Edition). London: Sage Publications
- Levin, J., Fox, J.A. and Forde, D.R. (2010). *Elementary Statistics in Social Research*. (11 Ed.). Boston: Pearson.
- Mallery, J. (2009). Building a secure organisation. In J.R. Vacca (Eds.), *Computer and Information Security Handbook*. USA: Elsevier Inc.
- Mead, N.R & Woody, C.C. (2017). *Cybersecurity Engineering: A practical approach for systems and software assurance*. USA:Pearson Education
- Miora, M., Kabay, M.E. & Cowens, B. (2014). Computer Security Incident Response Teams. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook*. 6<sup>th</sup> Edition. New Jersey: Wiley.
- Miora, M. (2014). Disaster Recovery. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook*. 6<sup>th</sup> Edition. New Jersey: Wiley.
- Mutai, E. (2018, December 9). Safaricom probed over costly M-Pesa outage. *Business Daily* [online]. Retrieved January 15, 2019 from <https://www.businessdailyafrica.com/news/Safaricom-probed-over-costly-M-Pesa-outage/539546-4888256-t7usb2z/index.html>
- NIST, (April, 2018). Framework for Improving Critical Infrastructure Cybersecurity. (V1.1). Retrieved January 25, 2019 from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

- Noble, K. (2009). Security through diversity. In J.R. Vacca (Eds.), *Computer and Information Security Handbook*. USA: Elsevier Inc.
- North, J., Pascoe, R., & Westgarth, C. C. (2016, April). *Cybersecurity and resilience —it's all about governance*. Retrieved 14 Dec, 2018 from [https://www.governanceinstitute.com.au/media/874783/cyber\\_security\\_resilience\\_governance\\_april\\_2016.pdf](https://www.governanceinstitute.com.au/media/874783/cyber_security_resilience_governance_april_2016.pdf)
- Olingo, A. (2018, July 14). *Two Kenyan banks lose \$0.86 million to hackers in a month*. The EastAfrican online Edition. Retrieved from <https://www.theeastafrican.co.ke/business/Two-Kenyan-banks-lose-to-hackers/2560-4663272-mfv6oy/index.html>
- Nuseir, M. (2010). The effect of e-service quality on customers' satisfaction in banks operating in Jordan: an empirical investigation of customers' perspectives. *International Journal of Services Economics and Management*. 2. 80-108. Retrieved May 15, 2019 from <https://www.researchgate.net/publication/317336193>
- Obura, F.( April 20, 2017). Kenya worst hit in East Africa by cyber crime. Retrieved July 16, 2019 from <https://www.standardmedia.co.ke/article/2001235820/kenya-worst-hit-in-east-africa-by-cyber-crime>
- Ombati, C. (2017, March 9). *Hackers steal Sh 30billion from Kenya's financial institutions*. East African Standard online. Retrieved from <https://www.standardmedia.co.ke/business/article/2001232042/hackers-steal-sh-30billion-from-kenya-s-financial-institutions>.
- Omer, M. (2014). *The resilience of networked infrastructure systems : analysis and measurement*. Singapore: World Scientific Publishing.
- Ormrod, D. & Turnbull, B. (2019). Modeling and Simulation Approaches. In A. Kott, & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks*. Switzerland: Springer.
- Oso, W.Y (2016). *Social Science Research:Principles and Practices*. Nairobi: The Jomo Kenyatta Foundation.
- Ponemon Institute. (2015, September). *The Cyber Resilient Organization: Learning to Thrive against Threats*. Retrieved 31 Dec, 2018 from [https://info.resilientsystems.com/hubfs/IBM\\_Resilient\\_Branded\\_Content/White\\_Papers/TheCyberResilientEnterpriseFinal\\_NorthAmerica.pdf?submissionGuid=c98689ce-de4f-4ff5-b457-f490e18bfa71](https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/TheCyberResilientEnterpriseFinal_NorthAmerica.pdf?submissionGuid=c98689ce-de4f-4ff5-b457-f490e18bfa71)
- Ponemon Institute. (2018a). *The Third Annual Study on the Cyber Resilient Organization*. Retrieved 31 Dec, 2018 from [https://public.dhe.ibm.com/common/ssi/ecm/55/en/55015655usen/the-3rd-annual-study-on-the-cyber-resilient-organization-white-paper\\_55015655USEN.pdf](https://public.dhe.ibm.com/common/ssi/ecm/55/en/55015655usen/the-3rd-annual-study-on-the-cyber-resilient-organization-white-paper_55015655USEN.pdf)
- Ponemon Institute.(2018b). *2018 Cost of Data Breach Study:Impact of Business Continuity Management*. Retrieved April 20, 2019 from <https://www.ibm.com/downloads/cas/4DNXZYWK>

- Ponemon Institute.(2018c). *Bridging the Digital Transformation Divide: Leaders Must Balance Risk & Growth*. Retrieved April 20, 2019 from <https://www.ibm.com/downloads/cas/ON8MVMXW>
- Rieger, C., Zhu, Q. and Başar, T.(2012, August 14-16). Agent-based cyber control strategy design for resilient control systems: Concepts, architecture and methodologies. Paper presented at the 2012 5th International Symposium on Resilient Control Systems, Salt Lake City, UT. doi:10.1109/VR.2006.148
- Rose, A., Miller, N., Eyer, J., and Banks, J. (2019). Economic effects of Mitigation and resilience. In A. Kott, & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks*. Switzerland: Springer.
- Rudolph, K. (2014). Implementing a security-awareness Program. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook*. 6<sup>th</sup> Edition. New Jersey: Wiley.
- SASRA. (July, 2018). *Licensed SACCOS*. Retrieved from <https://www.sasra.go.ke/index.php/regulation/licensed-saccos>
- Sekaran, U. & Bougie, R. (2009). *Research Methods for Business:A skill-building Approach*.(5<sup>th</sup> Edition). UK: Wiley & Sons.
- Serianu. (2015). *Kenya Cybersecurity Report 2015: Cyber Crime & Cybersecurity trends in Africa*. Retrieved September 22, 2018, from <http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf>
- Serianu. (2017). *Kenya Cybersecurity Report 2017*. Retrieved from <https://www.serianu.com/downloads/KenyaCyberSecurityReport2017.pdf>
- Sommestad, T.(2012). *A framework and theory for cybersecurity assessments*. Unpublished doctoral dissertation. Royal Institute of Technology, Stockholm.Security & Defence Agenda. (2013, December). *Cyber-Security: Problems outpace solutions*. Retrieved from <https://www.friendsofeurope.org/sites/default/files/media/uploads/2014/10/Cyber-security-report-2013-FINAL-Website1.pdf>
- Symantec. (2016, November). *Cyber Crime & Cybersecurity trends in Africa*. Retrieved September 22, 2018, from [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf)
- The Software Alliance Group. (2015). *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*. Retrieved from [http://cybersecurity.bsa.org/assets/PDFs/study\\_eucybersecurity\\_en.pdf](http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf)
- US CERT. (2016). *Cyber Resilience Review (CRR): Method description and self-assessment user guide*. Retrieved from <https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf>
- Whitman, M.E. & Mattord, H.J. (2014). *Management of Information Security*. (4th Ed). USA: Cengage Learning.
- Zikmund, W.G., Babin, B.J., Carr, J.C. & Griffin, M.(200). *Business Research Methods*. (8th Ed). USA: South-Western Cengage Learning.

## APPENDICES

**Table A-1 : Sources of indicators adopted for developing the cyber-resilience framework for Kenyan Banks.**

CERT-RMM	NIST	PONEMON	OTHERS, CBK	SERIANU	
1	Asset Definition and Management	Asset Management	Agility	Governance	Cybersecurity
2	Access Management	Business Environment	Security Posture	Training & Awareness	Vulnerability & threat management
3	Communications	Communications	Knowledgeable or expert staff	Incident Reporting	Governance & Strategy
4	Compliance	Risk Assessment	Leadership	Risk Mgmt & Assessment	Continuous monitoring & incident response
5	Controls Management	Risk Management Strategy	Planned redundancies	Outsourcing	
6	Environmental	Supply Chain Risk Management	Ample resources		
7	Enterprise Focus	Identity Management and Access Control	Preparedness		
8	External Dependencies Management	Awareness and Training			
9	Financial Resource Management	Data Security			
10	Human Resource Management	Information Protection Processes & Procedures			
11	Identity Management	Maintenance			
12	Incident Management and Control	Protective Technology			
13	Knowledge & Information Management	Anomalies and Events			
14	Measurement and Analysis	Security Continuous Monitoring			
15	Monitoring	Detection Processes			
16	Organizational Process Definition	Response Planning			
17	Organizational Process Focus	Governance			
18	Organizational Training and Awareness	Analysis			
19	People Management	Mitigation			
20	Risk Management	Improvements			
21	Resilience Requirements Development	Recovery Planning			
22	Resilience Requirements Management				
23	Resilient Technical Solution Engineering				
24	Service Continuity				
25	Technology Management				
26	Vulnerability Analysis and Resolution				
27	Generic Goals and Practices				

<b>Selected anchor framework</b>	
PONEMON (Current)	PONEMON (Adjusted)
Agility	Agility
Strong Security Posture	Strong Security Posture
Knowledgeable or expert staff	Knowledgeable or expert staff
Leadership	Leadership, <u>+Governance</u> and <u>+Compliance</u>
Planned redundancies	Planned redundancies
Ample resources	Ample resources
Preparedness	Preparedness
	<u>+ Asset classification and risk management</u>

## Appendix B – Consolidated List of Variables

**Table B-1: Consolidated List of Variables for measuring cyber-resilience**

<b>Part 1. Demographic information</b>	
<b>S1. What best describes your role or area of focus in the bank?</b>	
<input type="radio"/> IT security operations	
<input type="radio"/> IT operations	
<input type="radio"/> Cyber-security incident response team (CSIRT)	
<input type="radio"/> Business continuity management	
<input type="radio"/> None of the above	
<b>S2. Please check all the activities that you see as part of your job or role.</b>	
<input type="checkbox"/> Managing budgets	<input type="checkbox"/> Ensuring compliance
<input type="checkbox"/> Evaluating vendors	<input type="checkbox"/> Ensuring system availability
<input type="checkbox"/> Setting priorities	<input type="checkbox"/> None of the above
<input type="checkbox"/> Securing systems	
<b>S3. What best describes your position level within the bank?</b>	
<input type="radio"/> Corporate-level executive	<input type="radio"/> Supervisor
<input type="radio"/> Executive/CEO	<input type="radio"/> Staff/technician
<input type="radio"/> Director	<input type="radio"/> Administrative
<input type="radio"/> Manager	<input type="radio"/> Consultant/contractor
<input type="radio"/> Other (please specify) :.....	
<b>S4. What best describes your reporting channel or chain of command?</b>	
<input type="radio"/> CEO/executive committee	<input type="radio"/> Business unit leader or general manager
<input type="radio"/> COO or head of operations	<input type="radio"/> Head of compliance or internal audit
<input type="radio"/> CFO, controller or head of finance	<input type="radio"/> Head of enterprise risk management
<input type="radio"/> CIO or head of corporate IT	<input type="radio"/> Head of IT security
<input type="radio"/> Other (please specify): .....	
<b>S5. What best describes your organization's primary industry classification?</b>	
<input type="radio"/> Commercial Bank	



Mortgage Bank

Deposit Taking Micro Finance

Deposit Taking Cooperative Society

**S6. What range best describes the full-time headcount of your national organization?**

Up to 100

101 to 500

501 to 1,000

More than 1,000

## Part 2. Background Questions

**Q1a. In the past 2 years, did your organization have a data breach involving the loss or theft of money or data records containing sensitive or confidential customer or business information?**

Yes

No

Unsure

**Q1b. If yes, how frequently did these incidents occur during the past 2 years?**

Only once

2 to 3 times

4 to 5 times

More than 5 times

**Q2a. In the past 2 years, did your organization have a cybersecurity incident that resulted in a significant disruption to your organization's IT and business processes?**

Yes

No

Unsure

**Q2b. If yes, how frequently did these incidents occur during the past 2 years?**

Only once

2 to 3 times

4 to 5 times

More than 5 times

**Q2c. In the past 2 years, did your organization experience any of these security threats? (More than one choice allowed)**

Human error

IT system failures

Data exfiltration

Natural or manmade disasters

Advanced Persistent Threats (APTs)

Third- party glitches

Ransomware

Web site defacing/web site attack

Malicious Physical damage to equipment or infrastructure

Compromises based on Man-in-the-middle (MITM) attacks

**Q2d. Did any of the threats experienced above leak to public or press?**

Yes

No

Unsure



**Q15a. In the past 12 months, how has your organization's cyber resilience changed?**

Significantly improved  Improved  Somewhat improved  Declined  No improvement

**Q15b. If your organization has improved its cyber resilience, what caused the improvement? Please check your four top choices only.**

- Implementation of new technology, including cyber automation tools such as artificial intelligence and machine learning
- Elimination of silo and turf issues/non-knowledge sharing
- Visibility into applications and data assets
- Improved information governance practices
- Corporate-level buy-in and support for the cybersecurity and cyber-resilience programme
- Board-level reporting on the organization's cyber resilience
- Training and certification for IT security staff
- Training for end-users
- Hiring skilled personnel
- Engaging a managed security services provider
- Increased funding
- Regulatory enforcement

**Q16. In the past 12 months, how has the time to detect, contain and respond to a cyber-crime incident changed?**

- Time has increased significantly
- Time has increased
- Time has remained unchanged
- Time has decreased
- Time has decreased significantly

**Q17. What are the barriers to improving the detection, containment and response to a cyber-crime incident? Please check your top three choices.**

- Lack of Corporate-level buy-in and support for the cybersecurity function
- Lack of board-level reporting on the organization's state of cyber resilience
- Lack of training and certification for IT security staff
- Lack of training for end-users
- Inability to hire and retain skilled personnel
- Insufficient funding for the specific function

**18a. Please check one statement that best describes your organization's cybersecurity incident response plan (CSIRP).**

- We have a CSIRP that is applied consistently across the entire enterprise

We have a CSIRP, but is not applied consistently across the enterprise

Our CSIRP is informal or “ad hoc”

We don’t have a CSIRP

**Q18b. If you have a cyber-security incident response plan (CSIRP), how often is it reviewed and tested?**

Each month

Each quarter

Twice per year

Once each year

No set time period for reviewing and updating the plan

We have not reviewed or updated since the plan was put in place

**Q18c. If you have a Disaster Recovery (DR) plan, how often is it reviewed and tested?**

Each month

Each quarter

Twice per year

Once each year

No set time period for reviewing and updating the plan

We have not reviewed or updated since the plan was put in place

**Q18d. How do you rate your cyber-resiliency with regards to your Service level recoverability requirements to your customers in case of a disruption? Select one which closely represents this Bank.**

Continuous availability 99.999 percent Zero planned outages

Nearly continuous 99.99 percent Up to four-hour planned outages (maintenance)

High availability 99.9 percent Up to four-hour planned outages (maintenance)

Moderate availability 99.5 percent

**Q18e. How do you rate your cyber-resiliency with regards to your Service level objective to your customers in case of a disruption? Select one which closely represents this Bank.**

We want to return to service in less than five minutes (all events)

Local events return to service in less than five minutes; data centre return to service in less than two hours

All events to return to service in less than two hours

Local events: return to service in less than eight hours; data centre return to service in less than specified time frame (days to weeks)

**Q18f. How do you rate your *time to awareness* with regards to occurrence of a cyber-security incident?**

Outstanding

Good

Needs improvement

Inadequate

**Q18g. How do you rate your *time to response* with regards to occurrence of a cyber-security incident?**

Outstanding

Good

Needs improvement

Inadequate

**Q19a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?**

Yes

No

**Q19b. If your organization shares information about its data breach experience and incident response plans, what are the main reasons? Please select only three choices.**

Improves the security posture of my organization

Improves the effectiveness of our incident response plan

Enhances the timeliness of incident response

Reduces the cost of detecting and preventing data breaches

Fosters collaboration among peers and industry groups

Legal requirements

Other (please specify)

**Q19c. If no, why does your organization not participate in a threat-sharing program? Please select only two choices.**

Cost

Potential liability of sharing

Risk of the exposure of sensitive and confidential information

Anti-competitive concerns

Lack of resources

Lack of incentives

No perceived benefit to my organization

<input type="checkbox"/> Do not know about options to share intelligence					
<input type="checkbox"/> Other (please specify)					
<b>Q20. If yes, which of the following security technologies have been the most effective in helping your organization become cyber resilient. Please select your top seven choices.</b>					
<input type="checkbox"/> Web application firewalls (WAF)	<input type="checkbox"/> Data tokenization technology				
<input type="checkbox"/> Incident response platform	<input type="checkbox"/> Encryption for data in motion				
<input type="checkbox"/> Next generation firewalls	<input type="checkbox"/> Encryption for data at rest				
<input type="checkbox"/> Security information & event management (SIEM)	<input type="checkbox"/> Data loss prevention (DLP)				
<input type="checkbox"/> Cloud SIEM	<input type="checkbox"/> Virtual private networks (VPN)				
<input type="checkbox"/> Anti-virus / anti-malware	<input type="checkbox"/> Big data analytics for cybersecurity				
<input type="checkbox"/> Intrusion detection & prevention systems	<input type="checkbox"/> Distributed Denial of Service (DDoS) solutions				
<input type="checkbox"/> Network traffic surveillance	<input type="checkbox"/> Endpoint security solution				
<input type="checkbox"/> Identity management & authentication	<input type="checkbox"/> Governance solutions (GRC)				
<input type="checkbox"/> Code review and debugging systems	<input type="checkbox"/> User Behavioral Analytics (UBA)				
<input type="checkbox"/> Wireless security solutions	<input type="checkbox"/> Other (please specify)				
<b>Strongly Agree and Agree response:</b>					
<b>Please express your opinion about each one of the following statements using the agreement scale.</b>					
	Strongly agree	Agree	Moderate	Disagree	Strongly Disagree
Q21a. My organization's leaders recognize that enterprise risks affect cyber resilience.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Q21b. My organization's leaders recognize that cyber resilience affects revenues.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Q21c. My organization's leaders recognize that cyber resilience affects brand and reputation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Q21d. In my organization, funding for IT security is sufficient to achieve a high level of cyber resilience	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Q21e. In my organization, staffing for IT security is sufficient to achieve a high level of cyber resilience	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Q21f. My organization's leaders recognize that automation, machine learning, artificial intelligence and orchestration strengthens our cyber resilience.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Q22. Who has overall responsibility for directing your organization's efforts to ensure a high level of cyber resilience? Please check one choice only.</b>					

<input type="radio"/> Business continuity manager	<input type="radio"/> Chief technology officer (CTO)
<input type="radio"/> Business unit leader	<input type="radio"/> Chief risk officer (CRO)
<input type="radio"/> Chief executive officer (CEO)	<input type="radio"/> Chief information security officer (CISO)
<input type="radio"/> Chief information officer (CIO)	<input type="radio"/> No one person has overall responsibility
<input type="radio"/> Other (please specify)	
<b>Q23a. What is the full-time equivalent (FTE) headcount of your IT security function today?</b>	
<input type="radio"/> Less than 5	<input type="radio"/> 31 to 40
<input type="radio"/> 5 to 10	<input type="radio"/> 41 to 50
<input type="radio"/> 11 to 20	<input type="radio"/> 51 to 100
<input type="radio"/> 21 to 30	<input type="radio"/> More than 100
<b>Q23b. What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?</b>	
<input type="radio"/> Less than 5	<input type="radio"/> 31 to 40
<input type="radio"/> 5 to 10	<input type="radio"/> 41 to 50
<input type="radio"/> 11 to 20	<input type="radio"/> 51 to 100
<input type="radio"/> 21 to 30	<input type="radio"/> More than 100
<b>Q24. How long has your organization's current CISO or security leader held their position?</b>	
<input type="radio"/> Currently, we don't have a CISO or cybersecurity leader	
<input type="radio"/> Less than 1 year	
<input type="radio"/> 1 to 3 years	
<input type="radio"/> 4 to 6 years	
<input type="radio"/> 7 to 10 years	
<input type="radio"/> More than 10 years	
<b>Q25. What best describes the maturity level of the bank's cybersecurity program or activities?</b>	
<input type="radio"/> Early stage – many cybersecurity program activities have not as yet been planned or deployed	
<input type="radio"/> Middle stage – cybersecurity program activities are planned and defined but only partially deployed	
<input type="radio"/> Late-middle stage – many cybersecurity program activities are deployed across the enterprise	
<input type="radio"/> Mature stage – Core cybersecurity program activities are deployed, maintained and/or refined across the enterprise	
<b>Q26. Following are cybersecurity activities considered important by many organizations. Please rate each activity using the following scale:</b>	
<b>1 = implemented</b>	<b>2 = plan to implement in the next 12 months</b>

3 = plan to implement in more than 12 months

4 = no plan to implement

	Already Implemented 1	Planned within 12 months 2	Planned after over 12 months 3	No plan to Implement 4
Capture information about attackers (honey pot)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Conduct surveillance and fraud prevention	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Control endpoints and mobile connections	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Control over insecure mobile devices including Bring Your Own Device (BYOD)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Curtail end-user access to insecure Internet sites and web applications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Curtail unauthorized access to sensitive or confidential data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Curtail unauthorized access to mission-critical applications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Curtail unauthorized sharing of sensitive or confidential data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Curtail botnets and distributed denial of service attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Effort to reduce footprint of sensitive or confidential data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable adaptive perimeter controls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable efficient backup and disaster recovery operations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable efficient patch management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable multifactor authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable single sign-on	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish metrics or capability maturity model for management reporting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Limit access to insecure networks (e.g., public WiFi)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Limit the loss or theft of data-bearing devices (including IoT, detachable storage)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pinpoint and monitor anomalies in network traffic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pinpoint and monitor suspicious user behaviour (e.g., UBA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prioritize threats, vulnerabilities and attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide advance warning about threats and attackers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide intelligence about the threat landscape	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure access to cloud-based applications and infrastructure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure data stored in clouds	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use of machine learning and artificial intelligence for cybersecurity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



**Q27. Following are cybersecurity governance practices considered important by many organizations. Please rate each activity using the following scale: 1 = implemented, 2 = plan to implement in the next 12 months, 3 = plan to implement in more than 12 months, 4 = no plan to implement.**

	Already Implemented 1	Planned within 12 months 2	Planned after over 12 months 3	No plan to Implement 4
Hire and retain expert IT security personnel	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide clearly defined IT security policies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish and test backup and disaster recovery plans	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish business continuity management function	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish and test incident response management plan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Perform background checks of system users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Conduct specialized training for IT security personnel	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Conduct training and awareness activities for the organization's users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Monitor business partners, vendors and other third parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Conduct Internal or external audits of security and IT compliance practices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Segregate duties between IT and business functions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Perform risk assessment to evaluate IT security posture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adhere to standardized security requirements (ISO, NIST, COBIT, others)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Appoint a high-level security leader (CSO or CISO) with no more than 3 levels below the CEO and enterprise-wide responsibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Appoint a high-level leader (Chief Product Officer) accountable for information protection and privacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish a direct crisis communication channel to the CEO and board of directors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish a security program charter approved by executive management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Present to the CEO and board of directors on the state of cybersecurity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish a process for reporting cyber-crime and data breach to appropriate authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Purchase of cyber liability insurances	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establish metrics to evaluate the efficiency and effectiveness of IT security operations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fosters collaboration among peers and industry groups	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other (please specify in the spaces below, and provide rating)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

.....	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
<b>28 In this question, we want to understand what mostly drives the bank to invest in information (cyber) security. Using the following 10-point scale, please rate the following items from 1 = low to 10 = high.</b>					
	<b>1 or 2</b>	<b>3 or 4</b>	<b>5 or 6</b>	<b>7 or 8</b>	<b>9 or 10</b>
<b>28a.</b> Protection of information and data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28b.</b> Prevention of system outages/business process functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28c.</b> Compliance with security requirements imposed by authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28d.</b> Safeguard for reputation/ brand image	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28e.</b> Support for bank's business goals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28f.</b> Compliance with security requirements imposed by clients	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28g.</b> Enabler for digital transformation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28h.</b> Safeguard of humans	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>28i.</b> Increase of efficiency/cost reduction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Q29. Approximately, what is the dollar range that best describes your organization's current cybersecurity budget?</b>					
<input type="radio"/> Up to USD 1,000					
<input type="radio"/> USD 1,001 to 5000					
<input type="radio"/> USD 5,001 to 10,000					
<input type="radio"/> USD 10,001 to 15,000					
<input type="radio"/> USD 15,001 to 20,000					
<input type="radio"/> More than USD 20,000					
<b>Q30. Approximately, what percentage of the current cybersecurity budget will go to cyber resilience-related activities?</b>					
<input type="radio"/> < 2%	<input type="radio"/> 41% to 50%				
<input type="radio"/> 2% to 5%	<input type="radio"/> 51% to 60%				
<input type="radio"/> 6% to 10%	<input type="radio"/> 61% to 70%				
<input type="radio"/> 11% to 20%	<input type="radio"/> 71% to 80%				
<input type="radio"/> 21% to 30%	<input type="radio"/> 81% to 90%				
<input type="radio"/> 31% to 40%	<input type="radio"/> 91 to 100%				
<b>Q31. The following is a list of five areas of a cyber-security incident response plan (CSIRP). Out of 100%, please apportion approximately how much resources (time, money) your bank uses when prioritising each area.</b>					
Prevention	[	]	%		
Detection	[	]	%		
Containment	[	]	%		

Remediation	[       ]%
Post incident response	[       ]%
TOTAL	100%

**Q32. Some banks and other organisations have been implementing digital transformation. What is the current state of your digital transformation, if any?**

Completed    Going on now    Planned. Not yet started    Aware. Not Planned    Not aware

**Q33. What regulations are driving funding of your Bank's IT security? (More than one choice allowed).**

International laws by country

Kenya Banking Act

Cyber Regulations 2016/Computer Misuse and Cybercrime Act, 2018

Kenya Information Communication Regulations

Kenya Information Communication Act

EU General Data Protection Regulation (GDPR)

Sarbanes- Oxley

Other. (Please specify).....

**Q34. What is the status of the bank's cyber-risk insurance policy?**

We do not have

We are procuring

We have limited cover

We have a comprehensive cover

**Q35. We have an active compliance department**

Yes. Managed internally only

Yes. Outsourced only

Yes. Internally managed with outsourced expertise

We have no compliance department

**Q36. When serious cyber-crime incident happened, we:**

Did not report to law enforcers

Reported some cases

Reported to law enforcers who acted no further

Reported to law enforcers, who contacted the bank but acted no further

Reported to law enforcers who followed it up to successful prosecution

Reported to law enforcers who followed it up but with no successful prosecution

**Q37. In the past 12 months, which 2 of the following was the biggest cyber-crime impact experienced at the bank. Select only 2 most relevant.**

System downtime

Money Lost

No effect

Inconvenience

Reputation Damage

Psychological

**Q38. The bank manages and conducts the following security tests in-house: (More than one choice allowed).**

Vulnerability assessment  Security audit  Penetration Testing  Vulnerability assessment

**Q39. We conduct cybersecurity awareness training to our staff.**

Yes, it's compulsory  Yes, it's optional  No, we don't conduct.

**Q40. Some links in our website request for customer's personal identifying information.**

Yes  No  We do not maintain a website

**Q41a. We have an internal incident communication procedure:**

Yes  No  Not sure

**Q41b. Our staff understand and practice incident communication procedure:**

Yes  No  Not sure

**Q41c. We have an internalised crisis communication plan in the event of a cyber-attack.**

Yes  No  Not sure

**Q42. How do you see your cyber resilience posture in the next one year?**

Significantly improved

Somewhat improved

Remain the same

Somewhat worsen

Significantly worsen

**Table B-2: Frameworks, models and previous research instruments used in this research (Source: Author)**

<b>Name of Framework, model or instrument</b>	<b>Version</b>	<b>Description</b>
NIST Performance Measurement Guide for Info Security	V1.0	Provide metrics for verifying whether security controls are appropriately implemented
CERT Resilience Management Model (CERT-RMM)	1.2 (Feb, 2016)	CERT Resilience Management Model is a cyber-resilience framework developed by Carnegie Mellon University. It covers 27 categories/areas and metrics that need to be considered for a holistically resilient organisation.
Cyber Resilience Review (CRR) - Method description and self-assessment userguide	Feb 2016	Homeland Security Cyber Resilience assessment guide based on Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT®-RMM), both developed at Carnegie Mellon University's Software Engineering Institute.
Ponemon Institute: The Cyber Resilient Organization	2015, 2018	Research instruments developed and used by Ponemon Institute to measure cyber-resilience in organisations in UK, Germany, Australia, UAE, USA.
ISO/IEC 22301: Societal security–Business continuity management systems–Requirements	2012	These generic fit-for-all standards specify requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented system to protect against disruptive incidents
ISO/IEC 27001: Information technology -- Security techniques - Information security management systems -- Requirements	2013	These generic fit-for-all standards specify the requirements for managing information security within the context of an organization. It also spells out requirements for assessment and treatment of information security risks
ISO/IEC 27002: Information technology --Security techniques - Code of practice for information security controls	2013	These generic fit-for-all standards specify guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's prevailing information security risk environment.
ISO/IEC 27004: Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation	2016	Provides guidelines to assist organizations to evaluate information security performance and the effectiveness of information security management systems in order to fulfil the requirements of ISO/IEC 27001.
COBIT for Information Security	COBIT 5	Is a comprehensive risk management framework popularly used by organisations seeking global compliance.
The Centre on Local Government Research Framework by Rutgers University.	2019	Based on NIST

### Appendix C – List of variables grouped by Construct

Table C-1: List of variables grouped by Construct

Construct	Questions
Agility	q12bRating q12cRating q12dRating q12fRating q12gRating q12hRating q13aRating q14Rating q15aRating q15bRating q15cRating q15dRating q15eRating q15fRating q15gRating q15hRating q15iRating q15jRating q15kRating q15lRating q39Rating q51Rating
Ample Resources	q13fRating q31Rating q32Rating q36Rating q37Rating q56Rating
Asset Classification & Risk Profiling	q13hRating q35aRating q35bRating q35cRating q35dRating q35eRating q35fRating q35gRating q35hRating q35iRating q41Rating q45aRating q45bRating q45cRating q45dRating q45eRating q45fRating
Governance, Leadership & Compliance	q12iRating q12jRating q13gRating q17aRating q17bRating q17cRating q17dRating q17eRating q17fRating q25Rating q26aRating q26bRating q26cRating q26dRating q26eRating q26fRating q26gRating q26hRating q30aRating q30bRating q33Rating q40aRating q40bRating q40cRating q40dRating q40eRating q40fRating q40gRating q40hRating q42aRating q42bRating q42cRating q42dRating q42eRating q42fRating q42gRating q42hRating q42iRating q42jRating q42kRating q42lRating q42mRating q42nRating q42oRating q42pRating q42qRating q42rRating q42sRating q42tRating q42uRating q42vRating q42wRating q43Rating q44Rating q52Rating q53aRating q53bRating q53cRating q53dRating q53eRating q53fRating q53gRating q54aRating q54bRating q55aRating q55bRating
Knowledgeable or Expert Staff	q12jRating q13eRating q46aRating q46bRating q46cRating q46dRating q47Rating
Planned Redundancies	q13cRating q20Rating q21Rating q22Rating
Preparedness	q13bRating q16Rating q18Rating q19Rating q23Rating q24Rating q38aRating q38bRating q38cRating q38dRating q38eRating q48Rating q49Rating q50Rating

Strong Security Posture	q1Rating q2Rating q3Rating q4aRating q4bRating q4cRating q4dRating q4eRating q4fRating q4gRating q5Rating q6Rating q7aRating q7bRating q7cRating q7dRating q7eRating q7fRating q7gRating q7gRating q7hRating q7iRating q8Rating q9Rating q10Rating q11Rating q13dRating q27aRating q27bRating q27cRating q27dRating q27eRating q27fRating q27gRating q27hRating q27iRating q28aRating q28bRating q28cRating q28dRating q28eRating q28fRating q28gRating q28hRating q28iRating q28jRating q28kRating q28lRating q28mRating q28nRating q28oRating q28pRating q28qRating q28rRating q28sRating q28tRating q28uRating q28vRating q34aRating q34bRating q34cRating q34dRating q34eRating q34fRating q34gRating q34hRating q34iRating q34jRating q34kRating q34lRating q34mRating q34nRating q34oRating q34pRating q34qRating q34rRating q34sRating q34tRating q34uRating q34vRating q34wRating q34xRating q34yRating q34zRating
Perception to cyber-resilience	q12aRating q12eRating q29aRating q29bRating q29cRating q29dRating q29eRating q29fRating

**Table C-3: Cyber-resilience Mean scores per respondent per construct**

Respondent	Construct	Mean	Respondent	Construct	Mean
BNK018	1. Preparedness	4.57	BNK010	1. Preparedness	4.07
	2. Planned Redundancies	4.25		2. Planned Redundancies	3.5
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.29
	4. Governance, Leadership & Compliance	3.68		4. Governance, Leadership & Compliance	3.7
	5. Asset Classification & Risk Profiling	4.24		5. Asset Classification & Risk Profiling	3.94
	6. Ample Resources	3		6. Ample Resources	2.5
	7. Agility	2.82		7. Agility	2.41
	8. Strong Security Posture	2.87		8. Strong Security Posture	2.54
	9. Perception to Cyber-resilience	5		9. Perception to Cyber-resilience	4.75
BNK019	1. Preparedness	4.36	BNK012	1. Preparedness	3.71
	2. Planned Redundancies	3.75		2. Planned Redundancies	3.75
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.43
	4. Governance, Leadership & Compliance	3.85		4. Governance, Leadership & Compliance	3.74
	5. Asset Classification & Risk Profiling	4.12		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	2.67		6. Ample Resources	2.83
	7. Agility	2.59		7. Agility	3
	8. Strong Security Posture	2.82		8. Strong Security Posture	2.61
	9. Perception to Cyber-resilience	4.5		9. Perception to Cyber-resilience	5
BNK020	1. Preparedness	3.93	BNK013	1. Preparedness	4.07
	2. Planned Redundancies	2.5		2. Planned Redundancies	3.75



Respondent	Construct	Mean	Respondent	Construct	Mean
	3. Knowledgeable or Expert Staff	3.71		3. Knowledgeable or Expert Staff	4.43
	4. Governance, Leadership & Compliance	3.27		4. Governance, Leadership & Compliance	3.73
	5. Asset Classification & Risk Profiling	3.65		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	2.33		6. Ample Resources	2.67
	7. Agility	3.09		7. Agility	2.86
	8. Strong Security Posture	2.68		8. Strong Security Posture	2.73
	9. Perception to Cyber-resilience	4.25		9. Perception to Cyber-resilience	5
BNK021	1. Preparedness	4.29	BNK016	1. Preparedness	3.79
	2. Planned Redundancies	3.5		2. Planned Redundancies	3.25
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.43
	4. Governance, Leadership & Compliance	3.68		4. Governance, Leadership & Compliance	3.79
	5. Asset Classification & Risk Profiling	4.12		5. Asset Classification & Risk Profiling	4
	6. Ample Resources	3		6. Ample Resources	2.67
	7. Agility	2.64		7. Agility	2.68
	8. Strong Security Posture	2.65		8. Strong Security Posture	2.69
	9. Perception to Cyber-resilience	4.75		9. Perception to Cyber-resilience	4.25
BNK022	1. Preparedness	4.21	BNK002	1. Preparedness	4.07
	2. Planned Redundancies	3.5		2. Planned Redundancies	3.5
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.29
	4. Governance, Leadership & Compliance	3.74		4. Governance, Leadership & Compliance	3.7
	5. Asset Classification & Risk Profiling	4.12		5. Asset Classification & Risk Profiling	3.94
	6. Ample Resources	3		6. Ample Resources	2.5

Respondent	Construct	Mean	Respondent	Construct	Mean
	7. Agility	2.86		7. Agility	2.5
	8. Strong Security Posture	2.82		8. Strong Security Posture	2.71
	9. Perception to Cyber-resilience	5		9. Perception to Cyber-resilience	4.63
BNK023	1. Preparedness	3.79	BNK003	1. Preparedness	4
	2. Planned Redundancies	3.25		2. Planned Redundancies	3.25
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.43
	4. Governance, Leadership & Compliance	3.62		4. Governance, Leadership & Compliance	3.71
	5. Asset Classification & Risk Profiling	4.06		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	3		6. Ample Resources	2.67
	7. Agility	2.68		7. Agility	2.95
	8. Strong Security Posture	2.65		8. Strong Security Posture	2.81
	9. Perception to Cyber-resilience	4.75		9. Perception to Cyber-resilience	5
BNK024	1. Preparedness	4.07	BNK005	1. Preparedness	4.14
	2. Planned Redundancies	4.75		2. Planned Redundancies	3.25
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	3.86
	4. Governance, Leadership & Compliance	3.95		4. Governance, Leadership & Compliance	3.67
	5. Asset Classification & Risk Profiling	4.29		5. Asset Classification & Risk Profiling	3.88
	6. Ample Resources	3		6. Ample Resources	2.33
	7. Agility	2.82		7. Agility	2.41
	8. Strong Security Posture	2.95		8. Strong Security Posture	2.71
	9. Perception to Cyber-resilience	5		9. Perception to Cyber-resilience	4.63
BNK025	1. Preparedness	4.07	BNK007	1. Preparedness	3.79
	2. Planned Redundancies	4		2. Planned Redundancies	3.75

Respondent	Construct	Mean	Respondent	Construct	Mean
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.29
	4. Governance, Leadership & Compliance	3.59		4. Governance, Leadership & Compliance	3.82
	5. Asset Classification & Risk Profiling	4.12		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	2.5		6. Ample Resources	2.33
	7. Agility	2.59		7. Agility	2.68
	8. Strong Security Posture	2.65		8. Strong Security Posture	2.79
	9. Perception to Cyber-resilience	4.5		9. Perception to Cyber-resilience	4.75
BNK026	1. Preparedness	4.21	BNK034	1. Preparedness	3.93
	2. Planned Redundancies	3.5		2. Planned Redundancies	3.25
	3. Knowledgeable or Expert Staff	4.29		3. Knowledgeable or Expert Staff	4.43
	4. Governance, Leadership & Compliance	3.73		4. Governance, Leadership & Compliance	3.67
	5. Asset Classification & Risk Profiling	3.94		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	2.5		6. Ample Resources	2.33
	7. Agility	2.68		7. Agility	2.68
	8. Strong Security Posture	2.79		8. Strong Security Posture	2.81
	9. Perception to Cyber-resilience	4.63		9. Perception to Cyber-resilience	4.75
BNK027	1. Preparedness	3.93	BNK035	1. Preparedness	4.14
	2. Planned Redundancies	3.75		2. Planned Redundancies	3.5
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	3.86
	4. Governance, Leadership & Compliance	3.79		4. Governance, Leadership & Compliance	3.65
	5. Asset Classification & Risk Profiling	4		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	2.83		6. Ample Resources	2.33
	7. Agility	2.95		7. Agility	2.5

Respondent	Construct	Mean	Respondent	Construct	Mean
	8. Strong Security Posture	2.7		8. Strong Security Posture	2.54
	9. Perception to Cyber-resilience	5		9. Perception to Cyber-resilience	4.25
BNK028	1. Preparedness	4.21	BNK037	1. Preparedness	4
	2. Planned Redundancies	3.75		2. Planned Redundancies	4
	3. Knowledgeable or Expert Staff	4.29		3. Knowledgeable or Expert Staff	4.43
	4. Governance, Leadership & Compliance	3.8		4. Governance, Leadership & Compliance	3.8
	5. Asset Classification & Risk Profiling	3.59		5. Asset Classification & Risk Profiling	4.12
	6. Ample Resources	2.5		6. Ample Resources	2.83
	7. Agility	2.73		7. Agility	2.86
	8. Strong Security Posture	2.71		8. Strong Security Posture	2.65
	9. Perception to Cyber-resilience	4.75		9. Perception to Cyber-resilience	5
BNK030	1. Preparedness	4.36	BNK039	1. Preparedness	4
	2. Planned Redundancies	3.5		2. Planned Redundancies	3.5
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.29
	4. Governance, Leadership & Compliance	3.67		4. Governance, Leadership & Compliance	3.82
	5. Asset Classification & Risk Profiling	4.12		5. Asset Classification & Risk Profiling	4
	6. Ample Resources	2.5		6. Ample Resources	2.5
	7. Agility	2.73		7. Agility	2.68
	8. Strong Security Posture	2.76		8. Strong Security Posture	2.76
	9. Perception to Cyber-resilience	5		9. Perception to Cyber-resilience	4.75
BNK032	1. Preparedness	4.36	BNK040	1. Preparedness	4.29
	2. Planned Redundancies	4		2. Planned Redundancies	3.5
	3. Knowledgeable or Expert Staff	4.43		3. Knowledgeable or Expert Staff	4.43

<b>Respondent</b>	<b>Construct</b>	<b>Mean</b>	<b>Respondent</b>	<b>Construct</b>	<b>Mean</b>
	4. Governance, Leadership & Compliance	3.82		4. Governance, Leadership & Compliance	3.86
	5. Asset Classification & Risk Profiling	4.12		5. Asset Classification & Risk Profiling	4.18
	6. Ample Resources	2.83		6. Ample Resources	3
	7. Agility	2.91		7. Agility	2.73
	8. Strong Security Posture	2.64		8. Strong Security Posture	2.87
	9. Perception to Cyber-resilience	5		9. Perception to Cyber-resilience	5

## Appendix D -Descriptive Statistics for each Response question

**Table D-1: Descriptive Statistics for each Response question**

	N	Min	Max	M	SD
q1 What best describes the maturity level of the bank's cybersecurity program or activities?	26	2	5	3.85	1.12
q2 In the past 2 years, did the bank have a data breach involving the loss or theft of money or data records containing sensitive or confidential customer or business information?	26	2	4	2.15	0.543
q3 If yes, how frequently did these incidents occur during the past 2 years?	26	0	4	2.31	1.379
q4a Card systems	26	3	4	3.54	0.508
q4b Internet-based customer systems (e.g. internet banking)	26	3	4	3.31	0.471
q4c Internal core banking system	26	3	3	3	0
q4d Over-the-counter	26	3	4	3.08	0.272
q4e Mobile money systems	26	3	4	3.81	0.402
q4f Other systems (e.g. Cheque fraud, cash fraud)	26	3	4	3.65	0.485
q4g Not Applicable. No money was lost	26	3	4	3.08	0.272
q5 In the past 2 years, did the bank have a cybersecurity incident that resulted in a significant disruption to its IT and business processes?	26	2	4	2.31	0.736
q6 If yes, how frequently did these incidents occur during the past 2 years?	26	0	4	2.15	1.461
q7a Human error	26	2	4	2.15	0.543
q7b IT system failures	26	2	4	2.08	0.392
q7c Data exfiltration	26	4	4	4	0
q7d Natural or manmade disasters	26	4	4	4	0
q7e Advanced Persistent Threats (APTs)	26	2	4	3.77	0.652
q7f Third- party glitches	26	2	4	2.54	0.905
q7g Ransomware	26	2	4	3.92	0.392
q7g Web site defacing/web site attack	26	4	4	4	0
q7h Malicious Physical damage to equipment or infrastructure	26	4	4	4	0
q7i Compromises based on Man-in-the-middle (MITM) attacks	26	2	4	3.92	0.392
q8 Did any of the threats experienced above leak to public or press?	26	2	4	3.62	0.804
q9 In the past 12 months, how has the volume of cybersecurity incidents changed?	26	1	5	2.92	1.093
q10 In the past 12 months, how has the severity of security incidents changed?	26	1	5	2.15	0.967
q11 As a result of data breaches and cyber-crime incidents, how frequently do disruptions to business processes or IT services occur?	26	2	5	3.73	0.667

	N	Min	Max	M	SD
q12a The bank's cyber-resilience stature.	26	1	5	4.35	0.892
q12b The bank's ability to prevent a cyber-attack.	26	4	5	4.54	0.508
q12c The bank's ability to quickly detect a cyber-attack	26	4	5	4.5	0.51
q12d The bank's ability to contain a cyber-attack.	26	4	5	4.5	0.51
q12e The bank's ability to respond to a cyber-attack.	26	4	5	4.5	0.51
q12f How valuable cyber-resilience is to the Bank.	26	4	5	4.65	0.485
q12g The importance of having skilled cybersecurity professionals in your cybersecurity incident response plan (CSIRP).	26	4	5	4.62	0.496
q12h How difficult it is for the bank to hire and retain skilled IT security personnel	26	1	5	2.65	1.719
q12i The bank's ability to comply with the EU General Data Protection Regulation.	26	4	5	4.62	0.496
q12j Cybersecurity awareness among staff	26	4	5	4.73	0.452
q13a Agility	26	1	5	4.69	1.087
q13b Preparedness	26	1	5	4.69	1.087
q13c Planned redundancies	26	1	5	4.69	1.087
q13d Strong security posture	26	1	5	4.69	1.087
q13e Knowledgeable or expert staff	26	1	5	4.54	1.303
q13f Ample resources	26	1	5	4.69	1.087
q13g Governance, Leadership and Compliance	26	0	5	4.5	1.421
q13h Asset Classification and Risk Management	26	1	5	4.69	1.087
q14 In the past 12 months, how has your banks's cyber resilience changed?	26	4	5	4.5	0.51
q15a Implementation of new technology, including cyber automation tools such as artificial intelligence and machine learning	26	0	4	0.77	1.608
q15b Elimination of silo and turf issues/non-knowledge sharing	26	0	4	1.85	2.034
q15c Visibility into applications and data assets	26	0	4	2.92	1.809
q15d Improved information governance practices	26	0	4	1.23	1.883
q15e Corporate-level buy-in and support for the cybersecurity and cyber-resilience programme	26	0	4	1.23	1.883
q15f Board-level reporting on the organization's cyber resilience	26	0	4	0.15	0.784
q15g Training and certification for IT security staff	26	0	4	0.46	1.303
q15h Training for end-users	26	0	4	2.31	2.015
q15i Hiring skilled personnel	26	0	4	1.23	1.883
q15j Engaging a managed security services provider	26	0	4	0.92	1.719
q15k Increased funding	26	0	4	0.92	1.719
q15l Regulatory enforcement	26	0	4	2.62	1.941

	N	Min	Max	M	SD
q16 In the past 12 months, how has the time to detect, contain and respond to a cyber-crime incident changed?	26	1	5	3	1.233
q17a Lack of Corporate-level buy-in and support for the cybersecurity function	26	3	3	3	0
q17b Lack of board-level reporting on the organization's state of cyber resilience	26	3	3	3	0
q17c Lack of training and certification for IT security staff	26	3	3	3	0
q17d Lack of training for end-users	26	3	3	3	0
q17e Inability to hire and retain skilled personnel	26	3	3	3	0
q17f Insufficient funding for the specific function	26	3	3	3	0
q18 Please check one statement that best describes your organization's cybersecurity incident response plan (CSIRP).	26	4	5	4.88	0.326
q19 If you have a cyber-security incident response plan (CSIRP), how often is it reviewed and tested?	26	2	4	3.85	0.543
q20 If you have a Disaster Recovery (DR) plan, how often is it reviewed and tested?	26	2	4	3.92	0.392
q21 How do you rate your cyber-resiliency with regards to your Service level recoverability requirements to your customers in case of a disruption? Select one which closely represents this Bank.	26	2	5	2.73	0.919
q22 How do you rate your cyber-resiliency with regards to your Service level objective to your customers in case of a disruption? Select one which closely represents this Bank.	26	2	5	3.08	0.628
q23 How do you rate your time to awareness with regards to occurrence of a cyber-security incident?	26	0	5	4.08	0.935
q24 How do you rate your time to response with regards to occurrence of a cyber-security incident?	26	4	5	4.27	0.452
q25 Does this bank participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	26	2	5	4.88	0.588
q26a Improves the security posture of my organization	26	3	3	3	0
q26b Improves the effectiveness of our incident response plan	26	3	3	3	0
q26c Enhances the timeliness of incident response	26	3	3	3	0
q26d Reduces the cost of detecting and preventing data breaches	26	3	3	3	0
q26e Fosters collaboration among peers and industry groups	26	3	3	3	0
q26f Legal requirements	26	3	3	3	0
q26g Not Applicable - We do not share.	26	3	3	3	0
q26h Other (please specify)	26	3	3	3	0
q27a Cost	26	3	3	3	0
q27b Potential liability of sharing	26	3	3	3	0
q27c Risk of the exposure of sensitive and confidential information	26	3	3	3	0
q27d Anti-competitive concerns	26	3	3	3	0



	N	Min	Max	M	SD
q27e Lack of resources	26	3	3	3	0
q27f Lack of incentives	26	3	3	3	0
q27g No perceived benefit to my organization	26	3	3	3	0
q27h Do not know about options to share intelligence	26	3	3	3	0
q27i Other (please specify)	26	3	3	3	0
q28a Web application firewalls (WAF)	26	0	0	0	0
q28b Incident response platform	26	0	0	0	0
q28c Next generation firewalls	26	0	0	0	0
q28d Security information & event management (SIEM)	26	0	0	0	0
q28e Cloud SIEM	26	0	0	0	0
q28f Anti-virus / anti-malware	26	0	0	0	0
q28g Intrusion detection & prevention systems	26	0	0	0	0
q28h Network traffic surveillance	26	0	0	0	0
q28i Identity management & authentication	26	0	0	0	0
q28j Code review & debugging systems	26	0	0	0	0
q28k Wireless security solutions	26	0	0	0	0
q28l Data tokenisation technology	26	0	0	0	0
q28m Encryption for data in motion	26	0	0	0	0
q28n Encryption for data at rest	26	0	0	0	0
q28o Data loss prevention (DLP)	26	0	0	0	0
q28p Virtual private networks (VPN)	26	0	0	0	0
q28q Big data analytics for cybersecurity	26	0	0	0	0
q28r Distributed Denial of Service (DDoS) solutions	26	0	0	0	0
q28s Endpoint security solution	26	0	0	0	0
q28t Governance, Risk Compliance (GRC) solutions	26	0	0	0	0
q28u User Behavioral Analytics (UBA)	26	0	0	0	0
q28v Other (please specify)	26	0	0	0	0
q29a This bank's leaders recognize that enterprise risks affect cyber resilience.	26	5	5	5	0
q29b This bank's leaders recognize that cyber resilience affects revenues.	26	4	5	4.96	0.196
q29c This bank's leaders recognize that cyber resilience affects brand and reputation.	26	4	5	4.96	0.196
q29d In this bank, funding for IT security is sufficient to achieve a high level of cyber resilience	26	4	5	4.88	0.326

	N	Min	Max	M	SD
q29e In this bank, staffing for IT security is sufficient to achieve a high level of cyber resilience	26	4	5	4.69	0.471
q29f This bank's leaders recognize that automation, machine learning, artificial intelligence and orchestration strengthens our cyber resilience.	26	3	5	4.77	0.514
q30a Who has overall responsibility for directing the bank's efforts to ensure a high level of cyber resilience? Please check one choice only.	26	4	5	4.35	0.485
q30b Other (please specify)	26	0	0	0	0
q31 What is the full-time equivalent (FTE) headcount of your IT security function today?	26	0	0	0	0
q32 What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?	26	0	0	0	0
q33 How long has your organization's current CISO or security leader held their position?	26	3	5	4.46	0.905
q34a Capture information about attackers (honey pot)	26	3	5	4.62	0.804
q34b Conduct surveillance and fraud prevention	26	5	5	5	0
q34c Control endpoints and mobile connections	26	5	5	5	0
q34d Control over insecure mobile devices including Bring Your Own Device (BYOD)	26	3	5	4.92	0.392
q34e Curtail end-user access to insecure Internet sites and web applications	26	5	5	5	0
q34f Curtail unauthorized access to sensitive or confidential data	26	5	5	5	0
q34g Curtail unauthorized access to mission-critical applications	26	5	5	5	0
q34h Curtail unauthorized sharing of sensitive or confidential data	26	5	5	5	0
q34i Curtail botnets and distributed denial of service attacks	26	3	5	4.69	0.736
q34j Effort to reduce footprint of sensitive or confidential data	26	1	5	4.77	0.863
q34k Enable adaptive perimeter controls	26	0	5	4.5	1.175
q34l Enable efficient backup and disaster recovery operations	26	5	5	5	0
q34m Enable efficient patch management	26	3	5	4.92	0.392
q34n Enable multifactor authentication	26	1	5	4.54	1.174
q34o Enable single sign-on	26	1	5	1.69	1.49
q34p Establish metrics or capability maturity model for management reporting	26	1	5	4.23	1.394
q34q Limit access to insecure networks (e.g., public WiFi)	26	5	5	5	0
q34r Limit the loss or theft of data-bearing devices (including IoT, detachable storage)	26	3	5	4.69	0.736
q34s Pinpoint and monitor anomalies in network traffic	26	3	5	4.92	0.392
q34t Pinpoint and monitor suspicious user behaviour (e.g., UBA)	26	3	5	4.54	0.859
q34u Prioritize threats, vulnerabilities and attacks	26	3	5	4.92	0.392
q34v Provide advance warning about threats and attackers	26	3	5	4.69	0.736

	N	Min	Max	M	SD
q34w Provide intelligence about the threat landscape	26	3	5	4.69	0.736
q34x Secure access to cloud-based applications and infrastructure	26	1	5	2.54	1.816
q34y Secure data stored in clouds	26	1	5	2	1.523
q34z Use of machine learning and artificial intelligence for cybersecurity	26	1	5	2.54	1.63
q35a Protection of information and data	26	4	5	4.96	0.196
q35b Prevention of system outages/business process functionality	26	4	5	4.96	0.196
q35c Compliance with security requirements imposed by authorities	26	4	5	4.96	0.196
q35d Safeguard for reputation/ brand image	26	4	5	4.96	0.196
q35e Support for bank's business goals	26	4	5	4.85	0.368
q35f Compliance with security requirements imposed by clients	26	4	5	4.62	0.496
q35g Enabler for digital transformation	26	4	5	4.92	0.272
q35h Safeguard of humans	26	4	5	4.73	0.452
q35i Increase of efficiency/cost reduction	26	3	5	4.88	0.431
q36 Approximately, what is the dollar range that best describes the bank's current cybersecurity budget?	26	2	5	3.54	1.174
q37 Approximately, what percentage of the current cybersecurity budget will go to cyber resilience-related activities?	26	4	5	4.73	0.452
q38a Prevention	26	4	5	4.85	0.368
q38b Detection	26	3	5	4.69	0.549
q38c Containment	26	2	5	3.92	1.093
q38d Remediation	26	1	4	2.19	1.234
q38e Post incident response	26	1	4	1.85	1.156
q39 Some banks and other organisations have been implementing digital transformation. What is the current state of your digital transformation, if any?	26	3	5	3.92	1.017
q40a International laws by country	26	2	4	3.85	0.543
q40b Kenya Banking Act	26	4	4	4	0
q40c Cyber Regulations 2016/Computer Misuse and Cybercrime Act, 2018	26	4	4	4	0
q40d Kenya Information Communication Regulations	26	2	4	3.92	0.392
q40e Kenya Information Communication Act	26	2	4	3.85	0.543
q40f EU General Data Protection Regulation (GDPR)	26	2	4	3.85	0.543
q40g Sarbanes- Oxley	26	2	4	2.38	0.804
q40h Other (please specify)	26	2	2	2	0
q41 What is the status of the bank's cyber-risk insurance policy?	26	2	5	2.27	0.778
q42a Hire and retain expert IT security personnel	26	5	5	5	0

	N	Min	Max	M	SD
q42b Provide clearly defined IT security policies	26	0	5	4.81	0.981
q42c Establish and test backup and disaster recovery plans	26	5	5	5	0
q42d Establish business continuity management function	26	5	5	5	0
q42e Establish and test incident response management plan	26	5	5	5	0
q42f Perform background checks of system users	26	1	5	2.69	2.015
q42g Conduct specialized training for IT security personnel	26	3	5	4.92	0.392
q42h Conduct training and awareness activities for the organization's users	26	5	5	5	0
q42i Monitor business partners, vendors and other third parties	26	3	5	4.92	0.392
q42j Conduct Internal or external audits of security and IT compliance practices	26	5	5	5	0
q42k Segregate duties between IT and business functions	26	5	5	5	0
q42l Perform risk assessment to evaluate IT security posture	26	5	5	5	0
q42m Adhere to standardized security requirements (ISO, NIST, COBIT, others)	26	0	5	4.81	0.981
q42n Appoint a high-level security leader (CSO or CISO) with no more than 3 levels below the CEO and enterprise-wide responsibility	26	1	5	4.08	1.412
q42o Appoint a high-level leader (Chief Product Officer) accountable for information protection and privacy	26	1	5	1.92	1.623
q42p Establish a direct crisis communication channel to the CEO and board of directors	26	1	5	4.62	0.983
q42q Establish a security program charter approved by executive management	26	3	5	4.77	0.652
q42r Present to the CEO and board of directors on the state of cybersecurity	26	1	5	4.77	0.863
q42s Establish a process for reporting cyber-crime and data breach to appropriate authorities	26	0	5	4.73	1.041
q42t Purchase of cyber liability insurances	26	1	5	3.54	1.449
q42u Establish metrics to evaluate the efficiency and effectiveness of IT security operations	26	3	5	4.54	0.859
q42v Fosters collaboration among peers and industry groups	26	1	5	4.69	1.087
q42w Other (please specify and provide rating)	26	0	0	0	0
q43 We have an active compliance department	26	4	4	4	0
q44 In the past 12 months, when serious cyber-crime incident happened, we:	26	0	4	3.65	0.892
q45a System downtime	26	3	3	3	0
q45b Money Lost	26	3	3	3	0
q45c No effect	26	3	3	3	0
q45d Inconvenience	26	3	3	3	0

	N	Min	Max	M	SD
q45e Reputation Damage	26	3	3	3	0
q45f Psychological	26	3	3	3	0
q46a Vulnerability assessment	26	4	4	4	0
q46b Security audit	26	4	4	4	0
q46c Penetration Testing	26	4	4	4	0
q46d Vulnerability assessment	26	4	4	4	0
q47 We conduct cybersecurity awareness training to our staff.	26	5	5	5	0
q48 We have an internal incident communication procedure:	26	5	5	5	0
q49 Our staff understand and practice incident communication procedure:	26	5	5	5	0
q50 We have an internalised crisis communication plan in the event of a cyber-attack.	26	5	5	5	0
q51 How do you see your cyber resilience posture in the next one year?	26	4	5	4.92	0.272
q52 What best describes your role or area of focus in the bank?	26	5	5	5	0
q53a Managing budgets	26	0	4	3.85	0.784
q53b Evaluating vendors	26	4	4	4	0
q53c Setting priorities	26	4	4	4	0
q53d Securing systems	26	4	4	4	0
q53e Ensuring compliance	26	0	4	3.85	0.784
q53f Ensuring system availability	26	0	4	3.85	0.784
q53g None of the above	26	0	2	0.46	0.859
q54a What best describes your position level within the bank?	26	3	3	3	0
q54b Other (please specify)	26	3	3	3	0
q55a What best describes your reporting channel or chain of command?	26	3	3	3	0
q55b Other (please specify)	26	3	3	3	0
q56 What range best describes the full-time headcount of your national organization?	26	3	3	3	0
Valid N (listwise)	26				

### Appendix E – Map of Nairobi showing research locations.

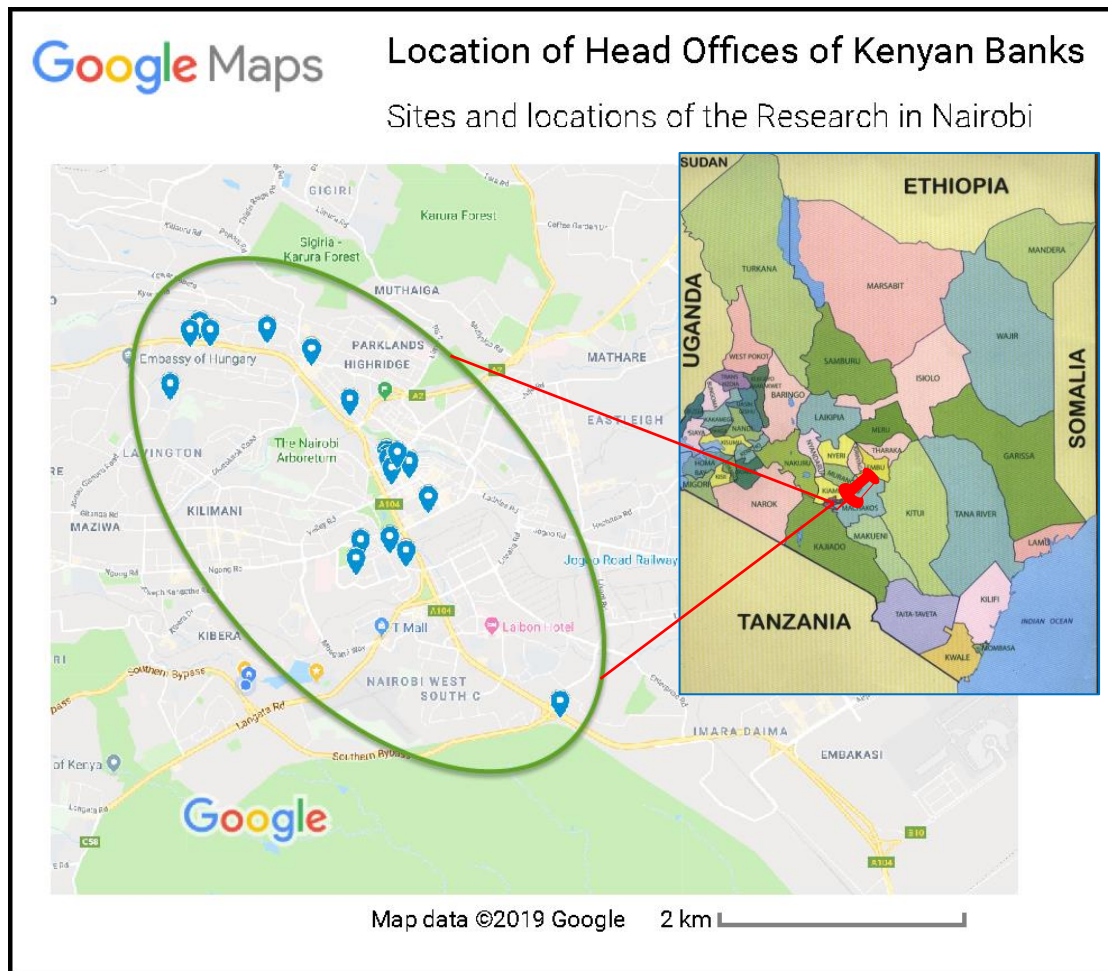


Figure E-1: Sites and location of research respondent banks in Nairobi Country. (Source: Google maps, 2019)

**Table E-1: List of banks sampled by the random sampler for the research** (Source: Kenya Bankers Association, 2019)


<b>List of sampled banks</b>				
<b>Original list No.</b>	<b>Bank Name</b>	<b>Peer Size</b>	<b>Sample No.</b>	<b>Research code No.</b>
14	Diamond Trust Bank (K) Ltd	Medium	13	1
12	Credit Bank Ltd	Small	11	2
40	Postbank	Small	33	3
43	Standard Chartered Bank (K) Ltd	Large	36	4
31	KCB Bank Kenya Ltd	Large	26	5
46	UBA Kenya Bank Ltd	Small	39	6
41	Rafiki Microfinance Bank	Small	34	7
30	Jamii Bora Bank Ltd	Small	25	8
11	Co-operative Bank of Kenya Ltd	Large	10	9
33	Mayfair Bank Ltd	Small	28	10
3	Bank of India	Medium	3	11
32	Kenya Women Microfinance Bank	Small	27	12
1	African Banking Corp. Ltd	Small	1	13
36	National Bank of Kenya Ltd	Medium	30	14
24	Guardian Bank Ltd	Small	22	15
44	SBM Bank (Kenya) Ltd	Small	37	16
47	Victoria Commercial bank Ltd	Small	40	17
9	Commercial Bank of Africa Ltd	Large	8	18
20	Family Bank Ltd	Medium	18	19
27	HFC Ltd	Medium	23	20
37	NIC Bank Ltd	Medium	31	21
34	Middle East Bank (K) Ltd	Small	29	22
38	Paramount Universal Bank Ltd	Small	32	23
8	Citibank N.A.	Medium	7	24
23	First Community Bank Ltd	Small	21	25
17	Ecobank Limited	Medium	15	26
10	Consolidated Bank of Kenya Ltd	Small	9	27
18	Spire Bank	Small	16	28

5	Barclays Bank of Kenya Ltd	Large	5	29
4	Bank of Baroda (K) Ltd	Medium	4	30
45	Transnational Bank Ltd	Small	38	31
42	Sidian Bank	Small	35	32
6	Stanbic Bank Ltd	Medium	6	33
21	Faulu Micro-Finance Bank	Small	19	34
13	Development Bank (K) Ltd	Small	12	35
22	Guaranty Trust Bank	Medium	20	36
16	Dubai Islamic Bank (Kenya) Ltd	Small	14	37
2	Bank of Africa Kenya Ltd	Medium	2	38
29	I & M Bank Ltd	Medium	24	39
19	Equity Bank Ltd	Large	17	40



**Appendix F – Research Permits.**

**Figure F-1: Research Permit by National Commission for Science, Technology and Innovation**

<p align="center"><b>THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013</b></p> <p align="center">The Grant of Research Licenses is guided by the Science, Technology and Innovation (Research Licensing) Regulations, 2014.</p> <p><b>CONDITIONS</b></p> <ol style="list-style-type: none"> <li>1. The License is valid for the proposed research, location and specified period.</li> <li>2. The License and any rights thereunder are non-transferable.</li> <li>3. The Licensee shall inform the County Governor before commencement of the research.</li> <li>4. Excavation, filming and collection of specimens are subject to further necessary clearance from relevant Government Agencies.</li> <li>5. The License does not give authority to transfer research materials.</li> <li>6. NACOSTI may monitor and evaluate the licensed research project.</li> <li>7. The Licensee shall submit one hard copy and upload a soft copy of their final report within one year of completion of the research.</li> <li>8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice.</li> </ol> <p>National Commission for Science, Technology and Innovation P.O. Box 30623 - 00100, Nairobi, Kenya TEL: 020 400 7000, 0713 788787, 0735 404245 Email: dg@nacosti.go.ke, registry@nacosti.go.ke Website: www.nacosti.go.ke</p>	 <p align="center"><b>REPUBLIC OF KENYA</b></p>  <p align="center"><b>National Commission for Science, Technology and Innovation</b></p> <p align="center"><b>RESEARCH LICENSE</b></p> <p align="center"><b>Serial No.A 22949</b></p> <p align="center"><b>CONDITIONS: see back page</b></p>
<p><b>THIS IS TO CERTIFY THAT:</b></p> <p><b>MR. MARICUS OTIENO MAYUNGA</b> <b>of AFRICA NAZARENE UNIVERSITY,</b> <b>0-200 NAIROBI, has been permitted to</b> <b>conduct research in Nairobi County</b></p> <p><b>on the topic: MODELLING AND VALIDATING A FRAMEWORK FOR ASSESSING CYBER-RESILIENCE OF KENYAN BANKS</b></p> <p><b>for the period ending:</b> <b>1st February, 2020</b></p> <p><b>Permit No : NACOSTI/P/19/20367/27925</b> <b>Date Of Issue : 1st February, 2019</b> <b>Fee Received :Ksh 1000</b></p> <div style="display: flex; justify-content: space-between;"> <div data-bbox="399 1612 606 1747">  <p><b>Applicant's Signature</b></p> </div> <div data-bbox="989 1321 1244 1590">  <p><b>Director General</b> <b>National Commission for Science, Technology &amp; Innovation</b></p> </div> </div>	

**Figure F-2: Research Permit letter by National Commission for Science, Technology and Innovation**



**NATIONAL COMMISSION FOR SCIENCE,  
TECHNOLOGY AND INNOVATION**

Telephone: +254-20-2213471,  
2241349, 3310571, 2219420  
Fax: +254-20-318245, 318249  
Email: dg@nacosti.go.ke  
Website : www.nacosti.go.ke  
When replying please quote

NACOSTI, Upper Kabete  
Off Waiyaki Way  
P.O. Box 30623-00100  
NAIROBI-KENYA

Ref. No. **NACOSTI/P/19/20367/27925**

Date: **1<sup>st</sup> February, 2019**

Maricus Otieno Mayunga  
Africa Nazarene University  
P.O. Box 53067-00200  
**NAIROBI.**

**RE: RESEARCH AUTHORIZATION**

Following your application for authority to carry out research on *“Modelling and validating a framework for assessing cyber-resilience of Kenyan Banks”* I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for the period ending **1<sup>st</sup> February, 2020.**

You are advised to report to **the County Commissioner and the County Director of Education, Nairobi County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit a **copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

*G. Kalerwa*

**GODFREY P. KALERWA MSc., MBA, MKIM  
FOR: DIRECTOR-GENERAL/CEO**

Copy to:

The County Commissioner  
Nairobi County.

The County Director of Education  
Nairobi County.

**Figure F-3: Research Approval letter by Africa Nazarene University**



**AFRICA NAZARENE**  
UNIVERSITY

January 18, 2019

To Whom It May Concern

Dear Sir/Madam,

**RE: PROPOSAL APPROVAL FOR MARICUS MAYUNGA (17M03DMIT006)**

The above named is a Master of Applied IT student at Africa Nazarene University. This is to confirm that his research proposal titled “**Modelling and validating a framework for assessing cyber-resilience of Kenyan banks**” has been approved for conduct of research, subject to obtaining other permissions and/or clearances that may be required beforehand.

Any support and/or assistance accorded to him will be highly appreciated.

Please feel free to contact me via email on [jobuhuma@anu.ac.ke](mailto:jobuhuma@anu.ac.ke) in case of further clarity required.

Yours Sincerely,



Obuhuma James

**Head of Department, Computer and Information Technology**

## Appendix G – Survey letters.

### Figure G-1: Letter to the banks requesting to participate in the research

February 21, 2019

ATTN: IT DEPARTMENT

~~XXXXXXXXXX~~

Via Email: ~~XXXXXXXXXX~~

Dear Sir/Madam,

#### **RE: Requesting to participate in a research study**

I am a student of Africa Nazarene University, Nairobi, pursuing a graduate programme leading to a degree in Msc. Applied Information Technology, with specialisation in Systems Security and Audit. I am conducting a thesis research on cyber resilience focusing on banks in Kenya. The research titled “*Modelling and validating a framework for assessing cyber-resilience of Kenyan Banks*”, aims at creating a localised qualitative framework for assessing cyber-resilience of banks. The output of the research will be, first, a new framework for assessing cyber-resilience, and second, application of the new framework to measure cyber-resilience posture of Kenyan banks.

The purpose of this letter is, therefore, to request your organisation to participate in this research by completing an online SurveyMonkey® questionnaire that will be sent to you once this initiation formality is completed. We request that the questionnaire respondent be a person accountable to cyber security/risk or information technology at the management level.

Utmost care has been taken to ensure that the questionnaire contains no information identifying the bank, staff, values or objects, are collected or stored with the research instruments or final report. The final report will be an aggregation rather than individual bank report. There will be no ranking of banks.

The proposed framework draws from standards (ISO/ISEC, NIST, COBIT, CERT-RMM), government/ military frameworks, successful empirical research on general resilience and cyber-resilience, cybersecurity, and a number of cyber security reports for Kenya and the world. The goal is to incorporate the best of breed measurements for this new cyber-resilience framework.

The final report could help bring confidence to Kenya’s financial sector, facilitate alignments in cyber resilience policies, and help stimulate development of new products like cyber-insurance.

I have attached all the requisite permits from National Commission for Science, Technology and Innovation (NACOSTI) and Africa Nazarene University approving this research. Should you require further clarification, please do not hesitate to contact the undersigned on ~~0111-208191~~ or the Africa Nazarene University faculty indicated hereunder.

Yours sincerely,



Maricus Mayunga (Student No. 17m03dmit006)

Africa Nazarene University research supervisors:

1. **Mr. J. Obuhuma, Chairman**, Department of Computer and Information Technology Phone: +254 ~~XXXXXXXXXX~~  
Email: ~~XXXXXXXXXX@anu.ac.ke~~
2. **Dr. K. Muchungi, Supervisor for this research**- Phone +254 ~~XXXXXXXXXX~~ Email: ~~XXXXXXXXXX@anu.ac.ke~~
3. **Dr. E. Roche, Supervisor for this research**- Phone +254 ~~XXXXXXXXXX~~ Email: ~~XXXXXXXXXX@anu.ac.ke~~

**Figure G2: How Survey link to Survey Monkey was distributed**

37. Survey URL
<a href="https://www.surveymonkey.com/r/fbfb990fdb986a4a9c7c812b9b36de74">https://www.surveymonkey.com/r/fbfb990fdb986a4a9c7c812b9b36de74</a>
QR Code


Survey URL 40

Survey URL
<a href="https://www.surveymonkey.com/r/474dcfe1022ec91a83757a1508a1a956">https://www.surveymonkey.com/r/474dcfe1022ec91a83757a1508a1a956</a>
QR Code