2022

An Assessment of the factors affecting cyber resilience in microfinance institutions in Kenya.

Kiganda, Moses
Strathmore Business School
Strathmore University

AN ASSESSMENT OF THE FACTORS AFFECTING CYBER RESILIENCE IN MICROFINANCE INSTITUTIONS IN KENYA

MOSES KIGANDA

ADMISSION NO. 136365

A Research Dissertation Submitted to the Strathmore Business School in Partial Fulfilment for the Degree of Master of Business Administration at Strathmore University

September 2022

DECLARATION

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Moses Edemba Kiganda

.....

Approval

The dissertation of Moses Edemba Kiganda was reviewed and approved for examination by the following:

Name of Supervisor: Dr Humphrey Njogu

Faculty Affiliation: Strathmore University Business School

Institution: Strathmore University

Dr. Angela Ndunge

Ag. Executive Dean

Strathmore University Business School.

Dr. Bernard Shibwabo

Director, Office of Graduate Studies

ABSTRACT

With the increased integration of new digital technologies in the financial industry, new risks and threats have emerged. One of the main threats to the operational efficiency and performance of financial institutions is the rise in cybercrimes which results in millions in losses annually. To curb this, institutions such as microfinance institutions (MFIs) have invested in cyber resilience practices. The current study sought to assess the various factors affecting cyber resilience in microfinance institutions in Kenya. The study specifically evaluated how management support, resource factors, and regulatory factors influence the cyber resilience in MFIs in Kenya. The research was guided by the resource-based view theory and the game theory. The examination was anchored on a positivist research philosophy with descriptive research guiding the study. The population for the examination was all the operational microfinance institutions in Kenya. The respondents for the survey were either the Chief Technology Officers, Chief Information Security Officers, or Technology Managers. A structured research questionnaire was adopted in the survey. The data collection for the study was done using Google forms and physical data collection where plausible. Data was analyzed using descriptive measures, correlation, and regression analysis. The findings of the study were presented using charts and tables. The research showed a positive relationship between the resource factors, regulatory factors, and management support with cyber resilience in MFIs in Kenya. The overall regression established that the selected factors contribute significantly to the cyber resilience state of MFIs in Kenya. The study recommends that to be more cyber resilient, the firms must be ready to allocate significant resources, both financial and technical to ensure that they meet the high costs associated with pursuing cyber resilience status. The study also recommends that managers align security decisions with organizational goals and capabilities to reduce organizational misalignment which can affect effective cyber resilience implementation. Lastly, policymakers in the MFI industry should assess the industry's readiness and develop a set of standards and regulations that all firms are capable of meeting as this would promote cyber resilience.

Keywords: cyber resilience, management support, resource factors, regulatory factors, microfinance

TABLE OF CONTENTS

DECLARATION ..... **III**

ABSTRACT ..... **IV**

TABLE OF CONTENTS ..... **V**

LIST OF TABLES ..... **VIII**

LIST OF FIGURES ..... **IX**

LIST OF ABBREVIATIONS ..... **X**

DEFINITION OF TERMS ..... **XII**

CHAPTER ONE: INTRODUCTION **1**

1.1 Introduction 1

1.2 Background of The Study 1

1.2.1 Cyber Resilience 4

1.2.2 Factors Affecting Cyber Resilience 5

1.2.3 Microfinance Institutions in Kenya 10

1.3 Statement of the Problem 10

1.4 Research Objectives 12

1.4.1 General Objective 12

1.4.2 Specific Objectives 12

1.5 Research Questions 12

1.6 Scope of Study 12

1.7 Significance of the Study 13

1.7.1 To policy markets 13

1.7.2 To microfinance firms 13

1.7.3 To scholars 13

CHAPTER TWO **14**

LITERATURE REVIEW **14**

2.1 Introduction 14

2.2 Theoretical Review 14

2.2.1 Resource-Based View Theory 14
2.2.2 Game Theory 15
2.2.3 Cyber Resilience 17
2.3 Empirical Review 18
2.3.1 Management Support and Cyber Resilience 18
2.3.2 Resource Factors and Cyber Resilience 21
2.3.3 Regulatory Factors and Cyber Resilience 23
2.4 Summary of Research Gaps 26
2.5 Conceptual Framework 28

CHAPTER THREE 30

RESEARCH METHODOLOGY 30

3.1 Introduction 30
3.2 Research Philosophy 30
3.3 Research Design 30
3.4 Target Population and Sampling 31
3.4.1 Target Population 31
3.4.2 Sampling Design 31
3.5 Data Collection Instruments 31
3.6 Data Collection Procedures 32
3.7 Research Quality 32
3.7.1 Validity Tests 32
3.7.2 Reliability Tests 33
3.8 Data Analysis and Presentation 33
3.9 Ethical Considerations 34

CHAPTER FOUR 36

PRESENTATION OF RESEARCH FINDINGS 36

4.1 Introduction 36
4.2 Response Rate 36
4.3 Background Information 36

4.4 Descriptive Analysis 37
4.4.1 Management Support Factors 37
4.4.2 Resource Factors 39
4.4.3 Regulatory Factors 40
4.4.4 Cyber Resilience in Microfinance Institutions 41
4.5 Correlation Analysis 43
4.6 Regression Analysis 44
4.7 Chapter Summary 45

CHAPTER FIVE 47

DISCUSSION, CONCLUSION, AND RECOMMENDATION 47

5.1 Introduction 47
5.2 Discussion 47
5.2.1 Management Support and Cyber Resilience 47
5.2.2 Resource Factors and Cyber Resilience 49
5.2.3 Regulatory Factors and Cyber Resilience 50
5.3 Conclusions 51
5.4 Recommendations 53
5.5 Suggestions for Further Research 53
5.6 Limitations of the Study 54

REFERENCES 55

APPENDICES 61

Appendix I: Letter of Introduction to Microfinance Institutions 61
Appendix III: Population of MFIs for the Study (Source: (AMFI-K, 2020; CBK, 2020)) 67
Appendix IV: Ethics Review Approval 68
Appendix V: NACOSTI Research Licence 69

LIST OF TABLES

Table 2:1 Components of Game Theory 16
Table 2.2 Literature Gaps 27
Table 2.3 Operationalization of Variables 29
Table 4.1 Summary of Demographic Information 36
Table 4.2 Management Support Factors 38
Table 4.3 Resource Factors 39
Table 4.4 Regulatory Factors 40
Table 4.5 Cyber Resilience 42
Table 4.6 Correlation Matrix 43
Table 4.7 Overall Regression Summary 44
Table 4.8 Overall ANOVA Summary 44
Table 4.9 Overall Regression Coefficients 45

LIST OF FIGURES

Figure 2.1 Conceptual Framework 28

LIST OF ABBREVIATIONS

AMFI: Association for Microfinance Institutions

API: Application Programming Integration

ATM: Automated Teller Machines

BCG: Boston Consulting Group

CA: Communication Authority of Kenya

CBK: Central Bank of Kenya

CERT: Computer Emergency Response Team

CIISI-EU: Cyber Information and Intelligence Sharing Initiative

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COMFI: Credit-Only Microfinance Institution

DCI: Directorate of Criminal Investigation

DDoS: Distributed Denial of Service

ECOWAS: Economic Community of West African States

ENISA: European Union Agency for Cybersecurity

ERP: Enterprise Resource Planning

EU: European Union

FS-ISAC: Financial Services Information Sharing and Analysis Centre

FTE: Full-time Employee

GCI: Global Cybersecurity Index

GDPR: General Data Protection Regulation

HTTPS: Hypertext Transfer Protocol Secure

ICT: Information and Communications Technology

IMF: International Monetary Fund

IR: Incident Response

IS: Information Systems

ITU: International Telecommunication Union

KNBS: Kenya National Bureau of Statistics

MFB: Microfinance Bank

MFI: Microfinance Institution

NE: Nash Equilibrium

PII: Personal Identifiable Information

PSP: Payment Service Provider

SACCO: Savings and Credit Co-operative

SME: Small and Medium Enterprises

SWIFT: Society for Worldwide Interbank Financial Telecommunication

URL: Uniform Resource Locator

WAF: Web Application Firewall

WEF: World Economic Forum

WMFI: Wholesale Microfinance Institution

DEFINITION OF TERMS

Cyber-attack	This is an unauthorized intrusion into a computer system and its related networks (Curti, Gerlach, Kazinnik, Lee, & Mihov, 2019).
Cybercrime	An illegal activity(s) in which computers or computer networks are used as principal tool(s) for perpetuating violations of laws, rules, or regulations (Minnaar, 2021).
Cyber resilience	An organization's ability and capacity to withstand, recover from and adjust to the effects of cyber-attacks (Carías, Labaka, Sarriegi, & Hernantes, 2019).
Cybersecurity	The process of ensuring the safety of cyberspace from known and unknown threats (Holt, 2018). It is the collective application of strategies, security measures, plans, threat administration tactics, engagements, training, paramount practices, assurance, and expertise to protect an organization's digital assets and infrastructure (Efthymiopoulos, 2019).
Cyberspace	A global virtual environment that is set up on Information and Communications Technology (ICT) and involves the interconnection of computer networks where information is exchanged in real-time and stored (Kott & Linkov, 2021).
Endpoint hardware	These include mobile devices, laptops, desktop personal computers (PCs), and other equipment such as servers and networks (Affum, 2019).
Industry 4.0	The large-scale integration of ICT in industrial production (Lykou, Anagnostopoulou, et al., 2019).
Threat actor	Also called a malicious actor, is an entity that is responsible for creating incidents that impact or has the potential to impact an organization's cybersecurity (Van de Mark, 2020).

CHAPTER ONE: INTRODUCTION

1.1 Introduction

The context for this research project was described in this chapter. The chapter first presents a background to the topic of study, a short review of the variables under investigation, and a statement of the problem. It then presents the objectives and research questions. The chapter then ends with the scope of the study and its significance to various stakeholders.

1.2 Background of The Study

Cyberspace is a global virtual environment that is set up on Information and Communications Technology (ICT), involving the interconnection of networks where information is exchanged in real-time (Toapanta Toapanta et al., 2020). International Telecommunication Union (ITU) notes that 3.5 billion people are connected online with 44 zettabytes of data stored digitally utilizing technologies such as cloud computing. The increased usage of ICT has given life to new organizational possibilities such as e-government services and new economic and productive paradigms such as Industry 4.0 and the broader digital economy (ITU, 2020). Globalization has enabled governments and businesses to adopt ICT as an avenue for creating modern employment. Businesses are using information technology (IT) innovations to create new markets and gain a competitive advantage by having more interactions, reducing transaction costs, and having direct communication with customers (Chege et al., 2020).

By embracing IT, small and medium enterprises (SMEs) have been able to: innovate, leading to improved performance on both profitability and growth, level the competitive playfield with larger firms, and improve their customer responsiveness (Tohãnean, Buzatu, Baba, & Georgescu, 2020). The adoption of IT in the financial industry has led to the diminishing of brick-and-mortar banks. Emerging technologies such as crypto-currencies-inspired distributed systems, open Application Program Interface (API), and crowd-sourced identity systems have enabled the financial industry to become faster, safer, and cost-efficient (Bandopadhyaya & Yang, 2019). It is on this backdrop of IT adoption that ITU notes that to realize the full potential of the digital world, a trusted and safe cyberspace is fundamental (ITU, 2020).

Cybersecurity is the process of ensuring the safety of cyberspace from known and unknown threats (Ndeda & Odoyo, 2019). It is a form of e-protection that is backed by a framework policy. It is an interdisciplinary science between IT, entrepreneurship, and legal law (Efthymiopoulos, 2019). Ndeda & Odoyo (2019) further assert that cybersecurity is a collective application of strategies,

security measures, plans, threat administration tactics, engagements, training, paramount practices, assurance, and expertise to protect an organization's digital assets and infrastructure. Cybercrime is an unlawful activity(s) in which computers or computer networks are used as a principal tool for perpetuating violations of laws, rules, or regulations (van de Mark, 2020). Cyber-security aims to protect software and hardware infrastructure that is connected to the internet via businesses, governments, and other firms that coordinate with our governments (Roege et al., 2017).

Holt (2018) notes that the rapid increase in internet usage and digitization of economic activities have led to the emergence of new online criminal activities. Toapanta Toapanta et al. (2020) study note that apart from the increased usage of IT, other factors that have accelerated cybercrime include the low level of education resulting in more vulnerable victims due to inadequate internet experience, high unemployment rates, poor development of the legal framework, and inadequate security measures by individual organizations with SMEs more impacted. International Telecommunication Union (ITU, 2020) notes that in 2020, the COVID-19 pandemic influenced the increase in internet traffic by 30% compared to 2019, and this was driven by people connecting for telecommuting, remote working, and learning.

As per Global Cybersecurity Index (GCI), there is increased recognition of cybersecurity risk, which has been exacerbated by the COVID-19 pandemic (ITU, 2020). Research firm Canalys reported that in 2020, there was a 119% increase in known breaches, with 101 billion data records compromised, and a 60% rise in ransomware attacks (Canalys, 2021). Global losses due to cybercrime were estimated to have risen from US$1 trillion in 2020 to as high as US$6 trillion in 2021 (ITU, 2020). According to the Communications Authority of Kenya (CA) national cyber threat landscape reports for Kenya, in 2018, there were 51.9 million cyber threats reported, 2019 had 110.9 million cyber threats reported, which represents a 113.7% increase, and 2020 had 158.4 million cyber threats reported representing a 42.8% increase year over year (CA, 2019, 2020). According to Minnaar (2021), an increase in the number of inexperienced digital users during the pandemic has exposed multiple business ventures to cyber threats from extremely experienced cyber-criminals, especially in developing economies.

According to Ponemon Institute (2021), the top ten initial cyber-attack vectors in 2021 are: first is compromised credentials (responsible for 20% of breaches resulting in US$4.37 million in average total cost of breach); second is phishing (17% of breaches resulting in US$4.65 million in average total cost of breach); third is cloud misconfiguration (15% of breaches resulting in US$4.37 million

in average total cost of breach); fourth is vulnerability in third-party software (14% of breaches resulting in US$4.33 million in average total cost of breach); fifth is physical security compromise (9% of breaches resulting in US$3.54 million in average total cost of breach); sixth is malicious insider (8% of breaches resulting in US$4.61 million in average total cost of breach); seventh is accidental data loss or lost device (6% of breaches resulting in US$4.11 million in average total cost of breach); eighth is system error (5% of breaches resulting in US$3.34 million in average total cost of breach); ninth is business email compromise (4% of breaches resulting in US$5.01 million in average total cost of breach); and tenth is social engineering (2% of breaches resulting in US$4.47 million in average total cost of breach) (Ponemon Institute, 2021).

Gartner's (2021) report, the global cybersecurity spending of US$150.4 billion was distributed on application security (US$3.7 billion or representing 2.5% of the expected global cybersecurity spending), cloud security (US$841 million or 0.6%), data security (US$3.5 billion or 2.3%), identity access management (US$13.9 billion or 9.3%), infrastructure protection (US$23.9 billion or 15.9%), integrated risk management (US$5.5 billion or 3.6%), network security equipment (US$17 billion or 11.3%), other information security software (US$2.5 billion or 1.7%), security services (US$72.5 billion or 48.2%), and consumer security software (US$7 billion or 4.6%) (Gartner, 2021). In making cybersecurity investment decisions, cost-benefit analyses, organization risk appetite, and business trade-offs need to be factored in (Kissoon, 2020).

The cyber security threat landscape is constantly changing. In 2012, the top cyber threats were key loggers, hacking, and ATM skimming. In comparison, the top 3 threats in 2015 were ransomware, database transaction manipulation, and social engineering (Ferdinando, 2016). Some cyberthreats emerge from competing firms and even rival countries (cyber warfare) (Shad, 2019), and cyber attackers have moved to the cloud, with cyber criminals offering their services through digital channels (Kovanen, Nuojua, & Lehto, 2018). Despite evidence that cyber threats are on the rise, Apanja and Matabi (2021) are affirmative that Kenyan financial institutions are highly exposed to advanced forms of cyber attacks; and most are unequipped to withstand the implications associated with a major attack. According to Kigen, et al. (2015), local cybersecurity professionals should be guided by Sun Tzu's quote, which emphasizes the concept of situational awareness. "It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles." Local businesses need to be on high alert and consistently assess their security position, performance, and availability of their critical network assets (Kigen, et al., 2015). With cyber

criminals becoming more professional, most cyber attacks are difficult to detect, and security professionals have to focus on establishing cyber security situational awareness within their respective organizations. This study sought to assess the factors that affect cyber resilience among microfinance firms in Kenya.

1.2.1 Cyber Resilience

Cyber resilience is the ability of an organization to withstand, recover from and adjust to the effects of cyber-attacks (Dupont, 2019b). Carías et al. (2020) classify cyber resilience into ten domain areas of importance to an organization. These include governance, risk management, asset management, threat and vulnerability management, incident analysis, awareness and training, information security, detection, continuous monitoring, business continuity management, and information sharing (Carías et al., 2020). Dupont (2019b) notes that cybersecurity is a subset of cyber resilience and goes further to state that an organization cannot have cyber resilience without cybersecurity. Creado & Ramteke (2020) indicate that firm's ability to foresee, detect, withstand, and recover from unexpected situations and attacks on cyber resources is referred to as cyber-resilience. Colicchia et al. (2019) contend that cyber-resilience measures all aim to minimize the impact of cyber-attacks and enable the business to remain operational after attacks that may otherwise have adverse effects on the business continuity of unprepared organizations.

Carte's (2017) report conducted for SWIFT Institute (affiliated with Society for Worldwide Interbank Financial Telecommunication (SWIFT)) finds that cybersecurity remains to be one of the top risks that financial institutions face. The cyber threat landscape is expanding and getting more complex and sophisticated for financial institutions (Carter, 2017). PricewaterhouseCoopers (PwC) East Africa's 2019 banking survey ranked cybersecurity as the second top challenge for financial institutions, as identified by banking executives (PwC, 2020). Due to the increasing dependency on digital technologies, financial institutions have become leading targets for cybercriminals, state hackers, hacktivists, and disgruntled staff who are motivated by the anticipation of financial gain (Dupont, 2019). In a report by the Center for Strategic and International Studies (CSIS, 2022), financial institutions are the leading targets of cyber-attacks since they handle all the money. Further, these institutions are targeted by nation-states due to their strategic economic importance as sources of political and ideological leverage.

According to the World Economic Forum (WEF), the five key cybersecurity challenges in 2021 are: first is the complexity of digitalization which is highly dependent on software, hardware, cloud

infrastructure, machine learning, and artificial intelligence tools. Second is the fragmented and complex global regulations such as the General Data Protection Regulation (GDPR), Computer Misuse and Cybercrimes Act (2018), and Kenya Data Protection Act (2019), among others. Complying with these regulations may cause conflict in priorities and budget. The third is the dependence on third parties service providers. With connected devices expected to reach 27 billion in 2021, adoption of 5G telecommunication networks, the internet of things, and smart systems, there is more dependence on a few service providers who could end up being the weakest link for supply chain cyber-attacks. Fourth is the lack of cybersecurity expertise which should drive organizations to focus on talent development. Fifth is the difficulty in tracking cybercriminals. The possibility of detection and prosecution of cybercriminals is as low as 0.05% in the United States of America (World Economic Forum, 2021). Mayunga (2019) study finds that only 20% of reported cybercrime by Kenyan banks was concluded by authorities.

As per the Kenya cybersecurity report for 2020 by Serianu (2020), despite over 70% of the surveyed organizations with some cybersecurity best practices in place, the number of validated and escalated cyber threats rose from 7,180 in 2018 to 48,664 in 2019, representing a 678% rise year over year. Mayung's (2019) study on cyber resilience in Kenyan banks found that all the banks surveyed had cybersecurity measures in place, but still, 50% experienced a high volume of cybersecurity incidents, of which 81% were considered severe. Despite the rise in cyber threats, organizations will continue to adopt more digitalization, challenges of limited resources will continue to pressure spending reduction on cybersecurity tools, and organizations will continue to increase the use of third-party managed services (Serianu, 2020).

The traditional cybersecurity approach of preventing or stopping cyber-attacks is no longer sufficient due to the rapid changes in technology and sophistication of cyber threats, which then requires organizations to learn how to co-exist with cyber incident disruptions (Carías et al., 2020; Dupont, 2019b). Overcoming these challenges will require cyber resilience, which adds additional measures such as anticipating, detecting, withstanding, recovering, and evolving by learning from cyber incidents at three levels organization, technology, and people (Carías et al., 2020).

1.2.2 Factors Affecting Cyber Resilience

Muthinja and Chipeta (2017) posit that the key drivers to the adoption of technological innovations in the financial sector are the growth in the financial industry both in organization size and customer base, the need to reduce transaction costs, and internal constraints such as budget. The

financial industry has embraced innovations such as branchless banking solutions such as mobile banking, agency banking, internet banking, and automated teller machines (ATM) (Muthinja & Chipeta, 2017). The Kenyan financial sector has further adopted technologies such as WhatsApp banking, integration of core banking systems with telecommunication service providers, and other third-party transaction channels (Serianu, 2020). CBK notes that the increased digitalization, such as the adoption of cloud computing, has led to an increase in cyber risks such as data infiltration affecting data integrity, confidentiality, and availability and calls for appropriate mitigation measures to be implemented to avoid or minimize the risk (CBK, 2020).

Felton Jr (2021) is affirmative that multiple factors influence businesses' ability to attain cyber resilience, with poor owner knowledge and support for the development of cyber-defence strategies affecting strategic orientation. The study by Catota et al. (2018) on cybersecurity response capability by financial institutions in Ecuador identified four cybersecurity barrier categories, namely people, processes, technology, and externalities. On people, Catota et al. (2018) identified a lack of cybersecurity awareness, the small size of cybersecurity teams, and the lack of cybersecurity specialists as the main people barriers. On processes, Catota et al. (2018) find that a lack of high-quality cybersecurity training locally increases the cost of access to training internationally, and the unavailability of local support by cybersecurity vendors delays the resolution of support incidences. Gwala's (2016) study on barriers to implementation of national cybersecurity in South Africa finds there is a lack of information sharing mechanisms by stakeholders and ineffective cybersecurity awareness programs as the target audience is not well covered with content and communication channels. Kabanda et al. (2018) find that SMEs are reluctant to comply with regulations. Deloitte & FS-ISAC (2020) note that rapid business growth and expansion leave cybersecurity tracking behind among financial institutions.

Kabanda et al.'s (2018) study on South Africa's SMEs finds a lack of management support, poor attitude toward security, and inexperienced internet users with limited exposure to online risks as barriers to cybersecurity. Jerome Orji (2019) is affirmative that weak laws and poor ICT end-user awareness within the Economic Community of West African States (ECOWAS) regional area have resulted in increased threats to the firm's online security. Laban et al. (2021) assert that digital experts are effective human resources in building cyber-resilience through the development and optimization of new institutional frameworks, especially regarding the development of laws on cyber-crime prevention and combating and data control. Soikkeli et al. (2022) call for redundancy

planning to ensure that firms do not trade cyber-security costs with profits, with Abraham & Sims (2021) arguing that the cost of attacks and mitigating these attacks may become too much for institutions in lower-income nations. According to Kott & Linkov (2021), institutions' inability to measure their level of cyber resilience makes achieving it even harder.

Although financial institutions have increased investment in enhancing cybersecurity and cyber resilience, their failure to assess the true impact of cyber risks might impact their ability to develop effective cyber-resilience frameworks (Dupont, 2019c). Research on a firm's cyber readiness show exposure from a composite of internal and external factors. Muhati (2018) studied cyber resilience using leadership and regulatory environment factors, while Muraguri, Mwalili & Mose (2019) investigated cybersecurity readiness using cybersecurity policies, technical and logistical security competencies, and top management support. Chizanga, Agola & Rodrigues (2022) study showed that lack of cyber security awareness, cyber security training, and limited infrastructure and policies for ICT cyber security practices are the main factors determining cyber security readiness. These factors revolve around three recurring themes; management support, resource factors, and regulatory policies. This study assessed how these factors influence cyber resilience within microfinance organizations in Kenya.

1.2.2.1 Management Support

Management support refers to the direct involvement and push of high-level executives towards strategic goal realization (Zwikael & Meredith, 2019). It includes participating in the translation of policies and objectives into goals and projects (Ahmed & Philbin, 2022). According to Nyesemane (2021), the influence of managers is an important aspect of strategic goal execution since these individuals are usually in charge of making decisions that affect everyone in the organization. Mandal (2020) avers that to institute changes within an organization, managers must prepare the employees psychologically and explain the importance of the change and how it will affect the employees. The management plays an integral role in instituting changes, and in microfinance firms, the management support was instrumental in approving finances and other resources for cybersecurity resilience (Bagheri, 2020). Managers can also facilitate cybersecurity by providing training programs to employees, motivating employees towards adopting change practices, and reducing employee resistance to change (Kemper, 2019). Huang & Pearlson (2019) report that the management is responsible for communicating the importance of information security importance and promoting its commitment. Barham et al. (2020) report a strong influence

of management support on the adoption of innovative practices through internal competencies development.

According to Hsu et al. (2019), management support determines the level of willingness to adopt new technologies and service delivery, while Lo et al. (2021) report a positive effect of management support on knowledge sharing and transparency disclosures. Uchendu et al. (2021) are affirmative that top management plays a significant role in the development of a cyber-security culture. The study by Daud et al. (2018) revealed that management support determines cooperation and cyber-security compliance.

1.2.2.2 Resource Factors

Resources refer to the complete collection of money, staff, materials, and other assets that organizations can draw on strategically to realize their goals and function effectively. Henderson and Cockburn (2014) define resources as any asset or input of production, whether tangible or intangible, that an organization owns, controls, or has access to on a semi-permanent basis. Firms utilize resources in creating, producing, and offering products to a market (Ghapanchi et al., 2014). Technological systems use capital, materials, people, information, time, tools, and machines as the main resources. Companies utilize their resources to produce goods and services, realize a competitive advantage, and achieve service differentiation. According to Porter (1985), resources include all the assets, capabilities, knowledge information, and organizational processes that allow firms to achieve their desired goals and enhance organizational effectiveness (Diin Fitri et al., 2018).

Regarding technology, the acquisition of advanced technologies is hampered by budget constraints, and where some new technologies are acquired, implementation challenges exist due to skills gaps (Catota et al., 2018). The ease of access to powerful malware tools such as the leaked nation-state hacking tools and supporting infrastructure, which aids threat actors even with limited skills, keeps the cybercriminals one step ahead of the financial institutions (Dupont, 2019). SWIFT Institute notes that cyber threats to financial institutions are increasingly coming from insecure low-cost mobile and IoT devices outside their networks which call for new authentication and monitoring technologies (Carter, 2017). The integrations of core banking systems with telecommunication and other third-party service providers introduce new cybersecurity risks that need constant assessments (Serianu, 2020). Kabanda et al. (2018) find that ICT complexities, legacy systems, running of outdated software, use of pirated software, unique usage patterns such

as reliance on mobile technology for financial transactions, and increased use of wireless technologies complicate the attainment of cyber resilience in SMEs.

Deloitte and FS-ISAC (2020) find that financial institutions' cybersecurity is challenged by the rapid changes in IT and increasing complexities. Deloitte & FS-ISAC report notes that as financial institutions continue to adopt emerging technologies to innovate and develop new products, services, and digital channels, these have become critical enablers for cyber-attacks. Hence, embedding cybersecurity into new products and services and new channels needs to be a top priority (Deloitte & FS-ISAC, 2020).

1.2.2.3 Regulatory Factors

Regulations are the rules, laws, and policies that the government passes to control how businesses behave and operate (Srinivas et al., 2019). Regulatory factors define how complex systems are managed and follow a set of rules and trends (Tanczer et al., 2019). Regulations include all the requirements that the government sets for businesses and individuals to meet, such as licenses and reporting requirements, and they protect firms from unfair competition, promote sustainable pricing, ensure firms participate in green development, and promote safer workplaces and products (Srinivas et al., 2019). According to Lee & Shin (2018), firms that fail to meet regulatory requirements risk facing criminal penalties and damaged reputations. Government regulations are key drivers of cyber-security resilience, and North & Pascoe (2016) affirm that governance issues have been hampering companies' implementation of cyber-security policies. However, according to Efthymiopoulos (2019), cyber-security policies have to be redeveloped constantly to ensure that it reflects a region's practical needs to facilitate its security resilience and business continuity.

Externalities such as weak legal frameworks make it difficult to enforce and punish cybercrime (Catota et al., 2018). SWIFT Institute notes that as more people get online and begin to bank online, the weak cyber defences, high mobile penetration, and insufficient law enforcement is putting financial institutions in Asia, Latin America, and Africa at the top of the target list of cyber-criminal groups which will lead to more data breaches and losses (Carter, 2017). Kabanda et al. (2018) find that the limited understanding of the threat actors impedes the development of effective cybersecurity strategies. The low uptake of cyber insurance is a barrier to reducing the cost impact of cyber-attacks. Dupont's (2019) and Camill's (2017) studies note the important role played by insurance companies in lessening the opportunity cost burden of cyber-insecurity and recommend cyber insurance as a key risk management measure. Roege et al. (2017) aver that developing

guidelines for organizational resilience might bridge the gap from cyber-security to resilience. Despite the importance of cyber insurance, Serianu's (2020) report finds that only 17% of the surveyed organizations in Kenya had cyber insurance. Mayunga (2019) also finds that 90% of surveyed banks had no cyber insurance in place.

1.2.3 Microfinance Institutions in Kenya

Microfinance Institutions (MFIs) are MSMEs regulated and licensed under Micro-Finance Act CAP493D (2006) (KNBS, 2016). In this study, MFIs include the categories given by the Association for Microfinance Institutions - Kenya (AMFI-K) as microfinance banks (MFBs) which are regulated by the Central Bank of Kenya (CBK), Credit-Only MFIs (COMFIs), and Wholesale MFIs (WMFIs) which are self-regulated under AMFI-K (AMFI-K, 2020). Serianu (2020) further states that the Kenyan financial sector players include banks, MFIs, and Savings and Credit Cooperatives (SACCOs).

AMFI-K (2020) report notes that its membership in 2020 stood at 34 COMFIs and 3 WMFIs (2 WMFIs are based in Kenya, and 1 WMFI is based out of Kampala, Uganda). In 2020 the WMFIs had a total of Kenya shillings (KES) 6.336 billion Outstanding Loan Portfolio (OLP) issued on 147 loan accounts, while COMFIs had OLP of KES13.418 billion on 327,341 loan accounts for the 14 COMFIs who had shared their data (AMFI-K, 2020). According to CBK (2020) annual bank supervision report, there are 14 microfinance banks (MFBs) in Kenya regulated by CBK with a total asset base of KES 74.9 billion, customer deposits of KES 49.4 billion (which represents 1.2% of the 2020 banking sector deposits in Kenya), and loan portfolio of KES 44.2 billion on 219,400 loan accounts.

1.3 Statement of the Problem

Cyber threats are on the rise (Nallainathan, 2021). Canalys (2021) reports that globally in 2020, there was a 119% increase in known breaches with 101 billion data records compromised and a 60% rise in ransomware attacks. In Kenya, cyber threats have been on the rise, with 2019 CA reporting a 113.7% year-over-year increase and 2020 showing a 42.8% rise compared to 2019 (CA, 2019, 2020). In 2018 Cybercrime losses in Kenya were estimated to be US$295 million (Serianu, 2018). Global losses are estimated to reach US $6 trillion in 2021 (ITU, 2020). As per SWIFT Institute, the financial sector remains to be a top target of cybercrime motivated by the availability of money in the financial sector (Carter, 2017). Some of the contributing factors to the increased cyber incidents in the financial sector include the increase in dependency on digital

technologies and digitalization of financial services (Dupont, 2019a; Maurer & Nelson, 2020; Serianu, 2018), low investment in cybersecurity pillars of people, processes and technology (Catota et al., 2018; Kabanda et al., 2018; Muhati, 2018), the challenges in prioritization of risk areas (Deloitte & FS-ISAC, 2020; Maurer & Nelson, 2020); and lack of collaboration and information sharing (ENISA, 2021; Maurer & Nelson, 2020).

Financial institutions have been implementing different cybersecurity solutions, which include cybersecurity monitoring and operations, endpoint and network security, identity and access management, cybersecurity governance, application, and data protection measures, among others (Deloitte & FS-ISAC, 2020). The increased digitalization is, however, increasing the cyber risks presenting cybersecurity challenges in the financial sector (Deloitte & FS-ISAC, 2020). If this trend continues, Creado & Ramteke (2020) and Curti et al. (2019) are assertive that financial institutions will face increased risks from cyber-criminals, and the issue will remain a challenge. Previous studies have classified cybersecurity barriers under four main categories of people, processes, technology, and externalities (Catota et al., 2018; Peters et al., 2018). Studies such as Abeka et al. (2019), Mayunga (2019) & Njiru (2013) have focused on cybersecurity challenges in Kenyan banks and SACCOs. This study examined the cybersecurity barriers in MFIs under the three themes of management support, resources, and regulations.

Deloitte & FS-ISAC (2020) call for increased spending on cyber security, reporting the low spending on cyber security to be a major hindrance to secure systems. Gartner (2016) argues that although spending on cyber-security alone is insufficient in addressing cyber-security concerns, enterprises should be spending between 4% to 7% of IT budgets on cybersecurity. Choi et al. (2017) note that due to limited resources, companies need to consider trade-offs to gain an optimum return on investment in cybersecurity as they minimize the cyber risks, calling for the use of layered security measures for strategic IT assets. Governments are also guiding the institution of policy guidelines and the establishment of common practices and compliance requirements across industries, with Putranti et al. (2020) reporting that regulatory policies must be well thought out to promote cyber-resilience among SMEs. Linkov & Kott (2019) consider skilled cyber-conscious human capital to be a fundamental aspect of improving cyber-resilience, a sentiment that is shared by Matern et al. (2019), who aver that organizations have to ensure they acquire employees with IT skills and a strong sense of aversion to corruption.

The study by Linkov & Kott (2019) identifies the important role of the management in leading and directing the cyber-resilience effort, noting their influence on cultural orientation. It is certain that as cyber threats to financial institutions continue to escalate, organizations must formulate and adopt effective cyber-resilience strategies. However, while the studies above affirm that various factors are essential to facilitating cyber-resilience, there is limited literature on cyber resilience among microfinance institutions in Kenya. This study tried to fill this empirical gap by investigating the effect of three main factors; management support factors, resource factors, and regulatory factors, on cyber resilience among MFIs in Kenya.

1.4 Research Objectives

1.4.1 General Objective

The general objective of the study was to analyze the factors that influence the cyber resilience of microfinance institutions in Kenya.

1.4.2 Specific Objectives

The specific objectives of the study were:

i. To establish the effect of management support on the cyber resilience of microfinance institutions in Kenya.
ii. To determine the influence of resource factors on the cyber resilience of microfinance institutions in Kenya.
iii. To evaluate the effect of regulatory factors on the cyber resilience of microfinance institutions in Kenya.

1.5 Research Questions

i. What is the effect of management support on the cyber resilience of microfinance institutions in Kenya?
ii. To what extent do resource factors influence the cyber resilience of microfinance institutions in Kenya?
iii. What is the effect of regulatory factors on the cyber resilience of microfinance institutions in Kenya?

1.6 Scope of Study

The study focussed on the effect of management support, the influence of resource factors, and regulatory factors on the cyber resilience of MFIs in Kenya. The unit of analysis was MFIs which included the 14 MFBs regulated by the CBK, 2 WMFIs, and 34 COMFIs, which are self-regulated

under AMFI-K. The study utilized a descriptive design. The study respondents from whom quantitative data was collected are Chief Technology Officers, Chief Information Security Officers, and IT Managers. The theoretical scope was based on resource-based view theory and game theory. The study scope was confined to primary research data collection from June to July 2022. The research methodology applied was strictly quantitative guided by the structured research instrument used.

1.7 Significance of the Study

Canalys (2021) reports that cyber threats are rising globally, with 2020 recording a 119% year-over-year increase in known breaches with 101 billion data records compromised and a 60% rise in ransomware attacks. This poses an existential threat to many businesses. Therefore, this study's findings sought to be useful and helpful to the nation, microfinance firms, students, and other stakeholders as the country work toward maintaining a secure cyber economy.

1.7.1 To policymakers

This study will be key to policy development in Kenya as the information generated from the findings can be used to guide policymakers in formulating policies and strategies affecting cyber security awareness and management. The study provides information to security professionals that could be used to determine how to develop sustainable and flexible cyber security frameworks. Regulatory bodies such as CBK and membership bodies such as AMFI-K can also benefit from the study's findings which they can incorporate in their advisories to the entire financial sector.

1.7.2 To microfinance firms

This study focused on the internal determinants of cyber resilience and its findings are key in directing microfinance managers on the improvement strategies against malicious insiders and outsiders. The findings provide insight that could be useful to microfinance firm managers charged with protecting critical assets as they give direction on the necessary investments that would increase their organization's cyber resilience.

1.7.3 To scholars

To future researchers and academicians, the information generated in the course of study does enrich the body of knowledge on cybercrimes in the country and surrounding financial institutions. The study also identified research gaps and suggested areas that require further research to enhance the cyber security topic. In addition, this study will serve as a source of reference for future scholars and researchers.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

A literature review involves the organization of ideas and findings of value and writing them to provide the context and theoretical framework for research (Saunders et al., 2019). This chapter analysed supporting literature on cybersecurity resilience factors. Anchored on the Resource-based view theory and game theory, this section examined the effect of management support, resource factors, and regulatory factors on cyber-resilience. The literature review covered both theoretical literature and empirical literature.

2.2 Theoretical Review

This section discussed the theoretical foundations for this study. The study adopted a multi-theoretical approach anchored on the Resource-Based View (RBV) theory, which was supported by Game theory. According to the RBV, organizations must look within to determine sources of competitive advantage, which in this study was cyber resilience. The basic principle of the Game theory is that in any interaction involving individuals with varying goals, one player's payoff is contingent on the strategies implemented by the opposing player. This study proposed that since cyber resilience is a continuous activity aimed at enhancing an organization's ability to respond to continuous cyber threats, they must look within to develop competencies that enable them to continuously anticipate, react and learn from emerging risks. The RBV theory informed the independent variables, while the Game theory explored the nature of cyber resilience.

2.2.1 Resource-Based View Theory

The resource-based view (RBV) theory asserts that resources are the sources of firms' superior performance and that firms that possess the ability to exploit their unique bundles of resources will gain sustainable competitive advantage (Freeman et al., 2021). This theory emerged in the early 1980s and 1990s out of increased focus on attaining competitive advantage from the works of Wernerfelt (1984) ("The Resource-Based View of the Firm"), and Barney (1991) ("Firm resources and sustained competitive advantage"). Miller (2019) defines firm resources as all the assets, capabilities, structures, processes, attributes, competencies, knowledge, and information that a firm possesses and can utilize to realize strategic goals, improve efficiency, and enhance effectiveness. Proponents of the RBV argue that businesses must carry out internal analysis to

identify the resources that would be utilized as sources of competitive advantage (Chatzoglou et al., 2018). The RBV asserts that organizations are better placed to react to changes in their operating environment if they can exploit existing resources effectively.

After development, Barney (1991) generated a list of attributes that resources must meet to become sources of competitive advantage. Barney (1991) asserts that firm resources must be valuable, rare, imperfectly imitable, and organized to capture value. The RBV model attributes organizational success to its ability to exploit its unique resources and capabilities (Miller, 2019). According to Whitfield (2019), critics of this theory argue that although internal resources are important, it is important to investigate the effect of both internal and external determinants of superior organizational performance. It has also been argued that the RBV only applies to large firms (Solesvik, 2018). However, proponents argue that firms need resources and management competencies to recognize and exploit productive opportunities. Resources become valuable only when they can be properly utilized to implement strategies and realize organizational goals, and even create smart business operations (Chumphong et al., 2020).

The resource-based view informs this study's independent variables. According to the resource-based view, the leader brings perspectives, skills, and information to the organization, which contributes to shared understanding and strategic alignment of business processes. Nandi et al. (2020) conclude that technology-enabled supply systems can benefit significantly from the development of compatible cyber security technologies. In the study by Yusif & Hafeez-Baig (2021), organizational governance improved with effective legal frameworks, policy compliance, and adoption of good practices afforded increased societal acceptance and built legal recognition. The resource-based view thus recognizes management competence and support, resource quality, and regulatory policies as sources of competitive advantage for firms hoping to achieve cyber resilience.

2.2.2 Game Theory

Game theory involves studies of how more than one economic agent (known as players) make choices that result in outcomes driven by the preferences (or utilities) of those agents (Ross, 2021). A player's outcome is not only influenced by their actions but also by the choices of the other players, and hence, such situations are referred to as games (Pham, 2015). The player utilizes the information set available to make choices when playing a game which becomes the strategy of that player. When the players implement their strategies, their joint actions contribute to the game

outcomes. An outcome gives a payoff to each player, and since each player is considered rational, they choose a strategy that maximizes their payoff (Asgariazad, 2014).

Nash equilibrium (NE) occurs when no player can improve their payoff by changing their strategy even when given the strategies of all other players in the game. In a zero-sum game (involving just two players), one player can only be made better off by making the other player worse off in payoffs (Ross, 2021). At NE, each player's choice action needs to be the best response to what other players have chosen to result in their current outcome. If an outcome has already been designated to occur using a certain strategy, then no individual player would benefit by using a different strategy (Pham, 2015). Cybersecurity managers make the following considerations before selecting a strategy; the value of the asset to the organization, the level of consumer trust, costs of non-compliance, and the resources required to implement the new strategies. Cyber-criminals, on the other hand, consider the potential value of the compromised asset, resources, and skills required to carry out a successful attack and the risk of being caught. These factors determine an organization's ability to achieve cyber resilience. Chorghe et al. (2020) summarize the components of the game theory as per Table 2:1.

Table 0:1 Components of Game Theory

Components	Description
Game	Any scenario where in the result is influenced by the actions of multiple players.
Player	Any entity making deliberate decisions based upon the rules of a game.
Strategy	Series of actions that players will perform under a given circumstance, which may or may not occur in the game.
Payoff	Payoff is anything that a player incurs by arriving at a consequence. It can be in any form such as money, utility etc.
Information Set	The data available at any given point in a game.
Equilibrium	The stage where all the players have reached an outcome after making their decisions.

Source: (Chorghe et al., 2020)

Game theory shares similar concerns with cyber security in terms of how they are applied. Game theory describes multi-person decision scenarios where each player chooses actions that result in the best possible rewards for oneself while anticipating the rational actions of other players (opponents). Asgariazad (2014) notes that when applying game theory in cybersecurity, the strategy of the attacker is closely related to that of the defender (system administrator) and vice versa. Game theory collides with San Tsu's emphasis on the importance of being situationally aware in that it stresses the importance of examining the number of possible threat scenarios in cyberspace (Ross, 2021). In both scenarios, the payoff is determined by how well prepared the defender is against the attacker. The success of a cybersecurity system depends on the defense strategies implemented by the defender (cybersecurity personnel) against the strategic actions taken by the attackers (threat actors); hence, it qualifies to be evaluated using the game theory framework as one player's outcome depends not only on their decisions but also on the opponents' choices (Asgariazad, 2014).

Using Game theory, we can develop a means for studying strategic steps undertaken to facilitate cyber resilience. Cotae et al. (2020) note that traditional cybersecurity strategies aimed to prevent known attacks. However, with the changing nature of cyber-criminals, game theory provides a means for analysing the continuous defense measures employed by different companies to counter cyber-attacks. This theory applies in this study due to the multi scenarios application of the theory, which should be useful in guiding system administrators and managers towards resource allocation in the ever-changing cyberspace, including the importance of managers' support in implementing strategies aimed at ensuring microfinance firms become cyber-resilience. The theory is also useful in explaining how organizations change policies and processes in response to the cyber security environment.

2.2.3 Cyber Resilience

Organizational cyber resilience refers to an organization's ability to prepare for, respond to and recover from cyber-attacks. The goal of cyber resilience is to ensure high-performance levels in an organization regardless of whether there is a cyber incident or not (Dupont, 2019b). Bellini and Marrone (2020) note that cyber resilience is not only about preventing a cyber breach but also about learning from the breach incident and adapting to changing cybersecurity conditions. Cyber resilience operationalization involves investment in preventive measures against known and

unknown cyber threats, planning for business continuity in the event of cyber incidents occurrence, cooperation with external parties such as information sharing entities, governance, cybersecurity awareness, and training (Carías et al., 2020).

Carías et al. (2020) posit that cyber resilience goes beyond traditional cybersecurity in three ways. First, cyber resilience aims at maintaining business continuity beyond the IT protection provided by cybersecurity. Second, cyber resilience goes up to business recovery and adaptation from cyber incidents, which acknowledges the co-existence of disruptive cyber incidents. The third is the broader approach toward multiple organizations instead of having a narrow approach to one organization. Dupont (2019b) notes that effective cybersecurity is a building block towards attaining cyber resilience, and according to Tsen et al. (2021), low cyber resilience results in a high number of successful cyber-attacks.

Carías et al. (2020) classify cyber resilience into 10 domain areas of importance that organizations should implement to facilitate effective cyber-security and improve cyber-resilience. These include governance, risk management, asset management, threat and vulnerability management, incident analysis, awareness and training, information security, detection with continuous monitoring, business continuity management, and information sharing.

2.3 Empirical Review

This section presented a review of previous researchers' findings on the relationships between the study variables. It first provided an overview of cyber resilience before resuming a review of literature explaining how management support, regulatory factors, and resource factors interact with cyber resilience.

2.3.1 Management Support and Cyber Resilience

2.3.1.1 IT Governance

Alina et al. (2017) researched the role of the internal auditor in cybersecurity resilience and asserted that management support for audit functions is significantly related to an organization's ability to detect, react to, and respond appropriately to cyber risks. The researchers adopted Deloitte's IIA Three lines of defense model with a view to cyber risks in their review. From this perspective, the researchers find that management plays a key role in cybersecurity management. In the first line of defense, they are responsible for creating a cyber-secure environment, anticipating risks, ensuring the independence of evaluators, and owning up to and managing risks. In the second stage, managers supervise the risk management quality and internal control systems

through facilitating communication and coordination operations. In the third stage, they influence the level of independence of the auditors, thus improving the organization's ability to manage known and unknown risks. The study fails to examine how regulations and resource availability impact cyber-security resilience. This study established how these factors interact and their impact on cyber resilience.

Lykou et al. (2019) investigated cyber resilience challenges within the airline industry, affirming that the sector is one of the most interconnected in the world. The study was guided by factors under the resilience umbrella. The research identified cyber-terrorists and nation-state actors as the most significant threats to air traffic management. Cybercriminals and insiders only presented medium threats. Managers' coordination capabilities influenced the level of cooperation between a wide range of security disciplines, such as information security, aircraft security, financial security, and control centre security. Managers played key roles in developing a structural and procedural basis for continuous intra-and inter-organizational cyber resilience analysis, managing interdisciplinary cyber-risk analysis teams, developing and maintaining a portfolio of cyber-threat scenarios, and creating consistency and synergy in safety and security. This study focused on cyber resilience in the airline industry. The current study focused on the financial industry.

Jensen (2015) investigated cyber resilience in the maritime industry to identify immediate and long-term steps for firms in the industry to adopt. The study finds that maritime operations are under the control of different entities, including banks, ports, customs offices, truckers, shared service centres, and information control centres, all of which share unique IT infrastructure and adopt varied cybersecurity standards. Hence a poorly developed standardization in cybersecurity approach, the risk of adopting a counterproductive national approach, and the likelihood of a long and tenuous time implementing a mandatory global standard threaten maritime cyber resilience. The report affirms that maritime managers are essential in developing a set of best practices and guidelines and encouraging the development of long-term plans to introduce global cybersecurity standards. The study also assigned managers the role of encouraging cyber resilience through the adoption of the developed voluntary guidelines.

In Ghana, Affum (2019) investigated the country's foreign banks' cyber security practices. Specifically, the study aimed to determine whether the adopted practices and established policies and security directives influence awareness levels resulting in cyber resilience. The study employed multistage sampling and utilized regression and correlation analyses, and collected data

from departmental managers, IT managers, and employees. Analysis revealed that although a cyber security policy had been communicated, its implementation was limited, and the banks had failed to communicate the expected standards or policies guiding their adoption. The analysis also revealed that the banks had invested extensively in internal auditing, yet this study considers internal auditing to be reactive rather than proactive as cyber resilience promises. The study calls for policy development to mandate banks to increase cyber security awareness among staff and customers through seminars and conferences and to provide routine training programs.

2.3.1.2 Management Role in Resource Allocation

Hausken (2020) reviewed the literature on cyber resilience aspects in firms, organizations, and societies. The study sought after common cyber resilience definitions to distinguish between actors and identify the fundamental determinants of cyber resilience to map out its expected future. This review reported that management competency is key to determining the choice of technologies and tools that an organization adopts; and how these are, in turn, updated over time. The study also found that managers' approach to communication with collaborating cyber resilience partners in the development of appropriate resilience strategies influences their impact on cyber resilience over time. The researcher affirmed that managers must determine the value of resources allocated and efforts made towards ensuring organizational cyber resilience. Future challenges include the colossal attack surface of the Internet of Things, insufficient technologies, challenges handling big data, possible extensive societal trust in computers and software, and a deteriorating culture of ethics.

2.3.1.3 Employee Empowerment and ICT Structure

Matern et al. (2019) sought after human factor challenges to digitalization and cyber-resilience in public administration. The literature review revealed that the public sector's approach to cyber management was limited by poor cost estimation, high employee turnovers due to low payment, lack of coordination, and difficulties in attracting and retaining employees with the right skills. The researcher affirmed that managers play a key role in selecting organizational human resource (HR) strategies which determine the quality of new entrants into the organization and in planning the corporate ICT structure, which provides these employees with infrastructural and cultural support. The researchers identify the top leaders as the driving force behind institutional change and increased awareness regarding cyber resilience measures and also in instituting changes to address the retention of employees with the required skills. Efforts to increase solutions sharing

and to develop and implement appropriate legal requirements and ICT standards were recommended to boost institutional efforts. This study focused on cyber resilience among public sector firms.

Balakrishnan et al. (2018) explored strategies that improve the cyber resilience of business systems that consume large amounts of data. The study carried out a literature review which revealed that cyber resilience components could be categorized into sensing, resisting, and recovering. Analysis revealed that business managers were more risk-averse and tended to trust in an ecological approach to cyber resilience. It was, however, determined that having cyber-sensitive senior IT managers is one of the most significant first steps to improving cyber security resilience since the managers tend to apply a more systematic view of organizational cyber resilience. The study also found that employee awareness, the management's ability to formulate monitoring and detection procedures, a cyber resilience culture, external communication, and recovery planning were also identified as useful antecedents to cyber resilience. The study reviewed literature while the current collected primary data.

2.3.2 Resource Factors and Cyber Resilience

2.3.2.1 Technology Investments

Carías et al. (2019) sought to define a cyber resilience investment strategy in the industrial context. This study employed the system dynamics methodology in gathering opinions from experts on how to best invest in cyber resilience through interviews. Specifically, the study sought to determine whether investment should be split equally between personnel training and technical security or whether more should be invested in personnel training or technical security. Specific conclusions were that the higher the management awareness about the cyber attacks' success probability, the higher the investment in cyber resilience. The expert response revealed that investment in technologies is an essential determinant of the cyber resilience-building process, while both technical security and personnel training were key. The study affirmed that managers must increase investment in gaining reasonable technical security before investing in the improvement of employee cyber resilience training. Carías et al. study sought interview data from manufacturers' IT specialists and employed thematic analysis.

2.3.2.2 Technical Capacity

Lykou and Anagnostopoulou (2019) researched threat mitigation and cyber resilience controls in smart airports. The study reviewed recent literature and collected data through online surveys

involving airport IT personnel. Survey results revealed that although most of the respondents reported effective cybersecurity policies regarding the protection of IT, lack of awareness regarding the greatest risks and low internet connectivity limited cyber resilience effectiveness. Further, legal gaps, the airport's failure to restrict access agreements with third parties, limited specialized security training, and failure to enforce rules on software installation, especially on employees' own devices, limited resilience. The respondents identified good technical practices, good organizational practices, and effective policies and standards as drivers of cyber resilience. Firewalls and network segmentation, user access, software and hardware updates, disaster recovery plans, and continuous monitoring of security and information security compliance from providers of external IT services were the most effective strategies. This study involved cyber resilience within the aviation industry.

Annarelli and Palombi (2021) sought to develop a conceptual framework for how firms can utilize their digitization capabilities for cyber resilience. The researchers achieved this through literature analysis. The analysis revealed that digitization improved organizations' online communication capabilities, promoted continuous learning and innovation capabilities, enabled the employment of heterogeneous resources, enabled environmental scanning, and allowed for timely reconfiguration of resources. These digitization capabilities were determined to be a pre-requisite in all stages of cyber resilience, from the planning, prevention, learning, and innovation to the adoption phase. The study affirms that it is important to possess a set of heterogeneous and diversified resources and competent leadership that can comfortably reconfigure these resources when necessary. This study was purely a literature review; the current study supplemented it with primary data.

Kasanga (2021) studied the outcomes of techniques employed by commercial banks to enhance cyber resiliency. The study employed an explanatory research design targeting 39 departmental heads in Kenyan banks' cybercrime departmental heads. Annual reports and questionnaires were used as sources of data. Multivariate regression and correlation analyses revealed that although traditional cyber security measures and technologies had been utilized, banks also employed privilege restriction, adaptive response, dynamic positioning, dynamic representation, analytic monitoring, coordinated protection, and substantiated integrity. All these positively influence cyber resilience effectiveness within commercial banks. However, the deception technologies as

additional cyber resilience tools had an insignificant impact on banks' cyber resilience. This study focused on commercial banks, while the current study investigated microfinance institutions.

2.3.2.3 Adequate Personnel

Employing the human–organization–technology (HOT) theory, Kumar et al. (2021) sought after the antecedents of enhanced organizational cyber-security. The study collected data from multiple IT specialists in various industries in India. The data collected were analyzed using the partial least squares-based structural equation modeling technique (PLS-SEM). Findings showed that the type of technologies used by an organization determines its level of cyber resilience. The legal consequences of non-compliance to regulations, the role of senior management, and information security standards were also significant determinants of organizational resilience. An organization's access to qualified technical specialists and the moral standing of its workforce are important determinants of long-term resilience. This was a multi-industry examination while the current investigated cyber resilience, specifically in the financial industry.

2.3.2.4 Financial Capacity

Akech et al. (2020) investigated county governments in Kenya in an examination of the role of county leadership and county employees in enhancing county cyber resiliency. Using a qualitative research methodology, 71 participants were selected using a random and purposive sampling technique. The study analysis revealed that established organizational rules and procedures impact overall county management and resilience. The study determined that county leaders play a key part in creating awareness regarding cyber security and approving financial resources for the realization of cyber resilience. County leaders were also reported to influence employee attitudes towards the issue, and through information security awareness, they increased employees' situational awareness. The study concluded that technical and financial resources, managerial competency, and compliance requirements influence cyber resilience within county governments.

2.3.3 Regulatory Factors and Cyber Resilience

2.3.3.1 Regulatory Guidelines

Bagheri and Ridley (2017) conducted a comprehensive review of previous literature on organizations' aspects that affect cyber resilience. The study was guided by Linkov & Kott's (2019) cyber resilience framework, which categorized cyber resilience into the physical, information, cognitive and social domains. Most literature emphasized planning and preparing, and absorption of the risks, while recovery and adoption to new operating conditions got the least attention.

Bagheri and Ridley affirmed that policy guidelines would provide an appropriate template that firms could utilize to select an active rather than a passive cyber resilience approach. Further, Bagheri and Ridley asserted that cyber threats could be addressed when managers position their work based on information, cognitive and social perspectives. In addition to legal framework development, their study found that managers have to place their organizations in positions that facilitate adaptation and adjustment to external developments. Bagheri and Ridley's paper explored previous researchers' literature findings and did not look at cyber resilience in microfinance.

Adu and Adjei (2018) looked into the influence of cyber security awareness and policies within Ghanaian corporations. The study utilized both quantitative and qualitative methodologies and utilized data from questionnaires and document analyses. 100 respondents who were involved in creating cyber security awareness and information policies were selected. The analysis showed that good IT knowledge is not an assurance for awareness of cyber security. Further, most firms were not implementing legal provisions into their information security policies. The study reported that the government must increase requirements for firms to create and enforce sustainable security awareness programs and policies, as this would increase employees' knowledge about internal organizational vulnerabilities. Further, Adu and Adjei asserted that the government has to develop policies that guide how firms access, use private data and react to data breaches while at the same time protecting the national IT infrastructure from threats. The methodology utilized by Adu and Adjei differed significantly from the techniques employed in the current study.

2.3.3.2 Legal Framework

Mughairi et al. (2019) sought to develop an innovative cyber security-based approach to improve the level of resiliency within Oman's national infrastructure. The paper adopted a qualitative methodology and used case studies to gain a better understanding of global cyber resilience approaches. The analysis showed that there is a rise in government-sponsored malware development, necessitating a national approach to designing a defense system with a multilevel architecture that enables the network to defend itself, detect, and dynamically respond to these new threats. It was determined that establishing National Computer Emergency Response Teams (CERT) provides cyber security advice and increases collaboration capacity among collaborating institutions and countries pursuing resilience of their critical infrastructures. Further, establishing legal requirements for critical service providers to have local security divisions dedicated to

upholding the system's integrity would improve national systems' cyber resilience. This study was based on the Omani national economy, while the current study focuses on cyber resilience for MFIs in Kenya.

Karabacak et al. (2020) sought an approach to designing an effective public-private partnership for enhancing cyber resilience in the space industry. The paper drew on findings from two PhD studies and affirmed that the growing cyberspace industry has multiple deficiencies and inconsistencies that have increased the industry's exposure to cyber risks. Further, the involvement of private sector companies in the cyberspace market has reduced investment into cyber security as these firms are mainly profit-oriented. The study affirms that the government plays a key role in sensitizing the private sector about the need for improving cyber resilience through the establishment of clearly defined governance mechanisms. The researchers find that nationalized approaches such as the provision of incentives like the provision of commercial benefits, regulation, and security support would improve cyberspace resilience. The study concludes that adopting a mixed approach would suffice if private players were directed by clearly defined policies and acquired resiliency-focused leaders. The government's incentives, strategies, and partnership plans should be employed harmoniously to improve the effectiveness of cybersecurity efforts.

2.3.3.3 Cyber Information Sharing

Karabacak and Tatar (2017) investigated cyber resilience efforts in Turkey using a literature review and institutional findings on the concepts of cyber maturity. The study determined that it would be in the national interests to develop a critical infrastructure protection program that would direct inter-organizational cooperation efforts. The study determines that critical infrastructure protection programs should be current and consistently evolving activities that need revision and updating to enable a better response to new threats and to incorporate new national critical infrastructures that are composed of clearly defined policies, strategies, standards, and legislation. National cybersecurity programs should be designed to identify key risks to critical infrastructure, facilitate cooperation and collaboration routines and facilitate information exchange through the development of standards, policies, awareness training, and legal foundations. Collaboration was determined to be a prerequisite of national cyber maturity, with cyber mature states being determined to have a high rate of information sharing, executive support, involvement in education and awareness activities, high support for cyber research and development, and an overarching

cybersecurity strategy. Raising a country's cyber maturity had a positive relation with national and organizational cyber resilience. This study examined the cooperation and collaboration by MFIs in facilitating cyber security information exchange.

2.3.3.4 Cyber Insurance

Dupont's (2019) and Camillo (2017) studies noted the important role played by insurance companies in lessening the opportunity cost burden of cyber-insecurity and recommend cyber insurance as a key risk management measure. The low uptake of cyber insurance was identified to be a barrier to reducing the cost impact of cyber-attacks. Roege et al. (2017) averred that developing guidelines for organizational resilience might bridge the gap from cyber-security to resilience. Despite the importance of cyber insurance, Serian's (2020) report found that only 17% of the surveyed organizations in Kenya had cyber insurance. Mayunga (2019) also found that 90% of surveyed banks had no cyber insurance in place. This study evaluated the uptake of cyber insurance by MFIs in Kenya.

2.4 Summary of Research Gaps

These studies show a significant influence of various factors on cyber resilience. However, these studies failed to investigate the specific context that the current research sought to examine, hence presenting a gap that this research sought to fill. Most of these studies were not carried out in Kenya such studies include Carías et al. (2019), and Annarelli and Palombi (2021). While Alina et al. (2017) report the importance of management support in cyber enhancement, they fail to examine how financial resources and regulatory policies influence cyber resilience. Other studies were employed in industries that this study did not investigate, including Lykou, Iakovakis, et al. (2019), who investigated airline cyber resilience, and Kasanga (2021), who focused on commercial banks. The study by Jensen (2015) also investigated maritime cyber resilience. Further, studies such as Matern et al. (2019) and Bagheri and Ridley (2017) only reviewed secondary literature, while the current included fieldwork findings. None of the above studies focused exclusively on the combined influence of regulatory factors, resource factors, and management support on cyber resilience in the microfinance industry. This study filled the above gap. Table 2.1 below presents a summary of the gaps.

Table 2.2 Literature Gaps

Author	Title	Findings	Research Gap	Response to gap
Alina et al. (2017)	Internal audit role in cybersecurity.	Managers are influential in the choice of monitoring and evaluation strategies.	The study failed to investigate how resource factors and regulations impact a firm's cyber resilience	This study expanded the scope by assessing the impact of regulations and resource factors influencing cyber resilience
Lykou, Iakovakis, et al. (2019)	Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management.	Management support facilitates inter-organizational coordination control, thus enhancing cyber resilience.	The research was based on the airlines industry, while the current investigates the financial industry	This study addressed these factors within microfinance firms
Annarelli & Palombi (2021)	Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework.	The power to possess and reconfigure resources enhances cyber resilience	This study investigated the relationship between digitization and cyber resilience	This study expanded the scope to regulatory determinants
Akech et al. (2020)	A Framework Based on Institutional Theory to Aid in Cyber Resiliency in County Governments of Kenya.	Rules and procedures impact county governments' ability to implement resilience strategies	This study investigated cyber resilience in local governments and not in the financial sector	This study addressed cyber resilience in financial institutions
Carías et al. (2019)	Defining a cyber resilience investment strategy in the industrial internet of things context.	Higher leadership awareness about cyber security increases investment in cyber-resilience strategies	This study collected interview data and utilized thematic analysis of the industrial internet of things	The current study utilized a descriptive method
Karabacak & Tatar (2017)	From the National Cyber Maturity to the Cyber Resilience: The Lessons Learnt	The development of a critical infrastructure protection program would streamline	This study was specific to national cyber security systems	This study addressed the cyber resilience of MFIs in Kenya

from the Efforts of Turkey.	cyber resilience efforts and improve the organization's ability to formulate cyber resilience strategies	

Source: Researcher (2022)

2.5 Conceptual Framework

A conceptual framework consists of the building blocks of research theory, and it aids in explaining the different constructs of research work in a visual and or text form and their relationships (Bryman, 2016). It defines the relevant variables of the research, which include the independent variables, dependent variables, moderating variables, mediating variables, and control variables (Bryman, 2016; Rishad, 2019). In this study, the independent variables were management support, resource factors, and regulatory factors, and this study investigated how these variables affect cyber resilience within microfinance firms.

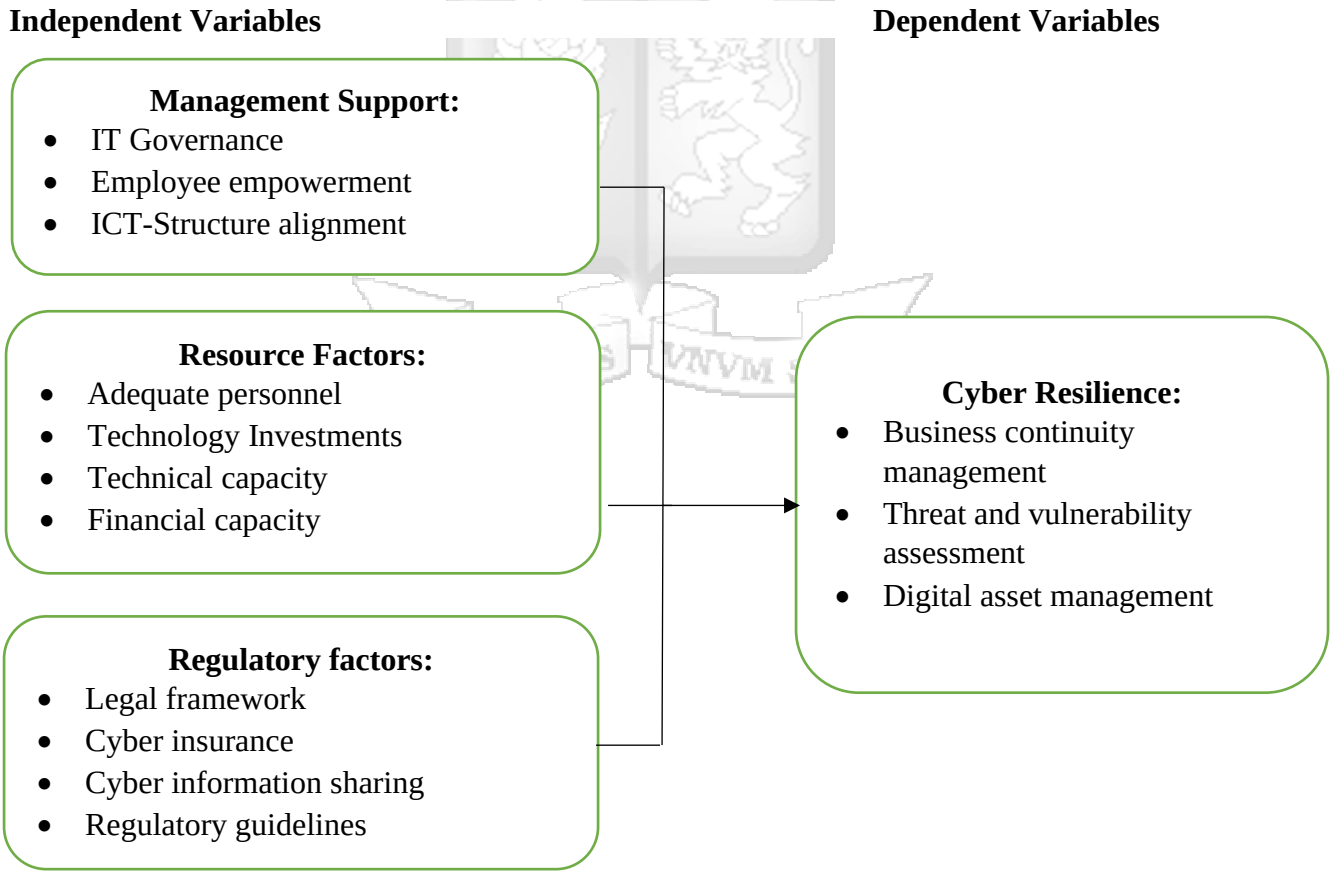

Figure 1.1 Conceptual Framework
Source: Researcher (2022)

The above conceptual framework identifies the illustrated relationship between management support, resource factors, and regulatory factors within microfinance institutions and how they impact the overall cyber resilience within the microfinance industry. The variables are operationalized as shown below in Table 2.2

Table 2.3 Operationalization of Variables

Variable	Indicators	Measurement	Data analysis
Management support	• IT Governance • Employee empowerment • IT-Structure alignment • Budget allocation	5-point Likert scale	Descriptive analysis and inferential analysis
Resource factors	• Adequate personnel • Technology Investments • Technical capacity • Financial capacity	5-point Likert scale	Descriptive analysis and inferential analysis
Regulatory factors	• Legal framework • Cyber insurance • Cyber information sharing • Regulatory guidelines	5-point Likert scale	Descriptive analysis and inferential analysis
Cyber resilience	• Continuity management • Threat and vulnerability assessment • Incident analysis • Continuous monitoring • Detection and management	5-point Likert scale	Descriptive analysis and inferential analysis

Source: Researcher (2022)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter covered the research methodology detailing research philosophy, research design, population and sampling, data collection, data analysis, research quality, and ethical considerations in the research.

3.2 Research Philosophy

Research philosophy is a system of assumptions and beliefs about the development of knowledge in a particular field. Positivism philosophy takes the view that the collection of data scientifically about an observable social phenomenon and searching for regularities and causal relationships lead to the creation of new generalizations (Saunders et al., 2019). The positivist ontology believes that the world is external and that there is a single objective reality to any research phenomenon or situation, regardless of the researcher's perspective or belief. The study employed a questionnaire as the measurement instrument to collect data on management support, resource factors, and regulatory factors within microfinance institutions and how they impact the overall cyber resilience within the microfinance industry.

3.3 Research Design

Research design provides a framework for organizing research work activities, such as the generation and collection of data that address the research questions. A quantitative study involves the collection of numeric data to show the relationship between theory and the observable social reality (Bryman, 2016). A descriptive study design was adopted in the current study as it allows for quantitative approaches to be used in the analysis of the research data. Moreso, the study design supports the examination of the study variable at a particular time with minimal intervention from the investigator, thus fostering neutrality in understanding how the variables interact with each other. Further, the descriptive research design was used in this study to quantitatively establish any relationship that exists between the independent and dependent variables of the study. The independent variables for this study are management support, resource factors, and regulatory factors. This study investigated how these variables affect the dependent variable, which is cyber resilience within microfinance firms.

3.4 Target Population and Sampling

3.4.1 Target Population

Bryman (2016) posits that a population is the universe of units from which a researcher wants to carry out an investigation. A unit of analysis in a study is the major entity that the researcher wants to be able to make conclusions on at the end of the study (Grünbaum, 2007). The unit of analysis for this study is the MFI in Kenya. MFIs in Kenya consist of 14 MFBs regulated by CBK, 2 WMFIs, and 34 COMFIs registered with AMFI-K, a total of 50 institutions (AMFI-K, 2020; CBK, 2020). The study respondents were the Chief Technology Officers (CIOs)/ Chief Information Security Officers (CISOs)/IT Managers in the registered MFIs in operation within Kenya.

3.4.2 Sampling Design

The study carried out a census of the entire study population which is 50 institutions. The study was done in two phases comprising the pilot phase and the main phase. Saunders et al. (2019) recommend a 95% confidence level with a margin of error of plus or minus 3% to 5% for business and management research. Saunders et al. further note that getting a 100% response rate is unlikely, and hence, the sample needs to be larger to ensure adequate responses for the required margin of error to minimize the risk of non-response bias and ensure that the sample is representative. However, owing to the small sample for the study and to fully enhance the response rate, this study used a census sampling that enhanced the response rate from all 50 microfinance institutions in Kenya. The use of census sampling ensured there was a full representation of the entire sample, thus fostering the generalizability of the research responses.

3.5 Data Collection Instruments

The study dominantly relied on primary research data that was collected using a structured research questionnaire. The questionnaire had closed-ended questions with multiple choices, single-choice, and matrix questions that used a five-point Likert scale. The questionnaire was used in the survey as it makes it easy to obtain information from a large population and applies a systematic approach in the data collection, which eases the tabulation and interpretation of the results. The Likert scale enabled the study to measure different dimensions and the degree of intensity of the respondents' attitudes on the items as they relate to MFIs' cyber resilience. This study used a five-point Likert scale where a score of 5 shows a respondent has a strong agreement with a 1, reflecting a strong disagreement.

3.6 Data Collection Procedures

This study's measurement instrument was a self-administered questionnaire that was distributed through Google forms, and physical data collection was plausible. The online questionnaires are less expensive and convenient to reach out to the respondents with a link to the survey being delivered through their official email addresses for reliability. An online survey is convenient for the respondents to fill in during their free time, from anywhere, and at their own pace; hence, likely to increase the response rate (Bryman, 2016). Where the respondents were unreachable online, printed questionnaires were delivered, and responses were obtained. The researcher and research assistant reached out to the respondents via phone to introduce the researcher and research objectives. Thereafter, the respondents who agreed to take part in the study were sent the online survey link through the respondents' institution's official email address. The respondent's official email address was the preferred means of sending the survey link to ensure reliability. The researcher and research assistant made follow-ups to the respondents who had not responded in a week from the time of sending out the questionnaire. The printed questionnaire was then used to get responses from those who did not return the online questionnaire.

3.7 Research Quality

The pilot phase covered 5 (10% of the sample) MFIs (2 MFB and 3 COMFIs) with 5 respondents who are Chief Technology Officers/IT Managers/ Chief Information Security Officers. The respondents involved in the pilot test were not included in the final research. The pilot survey feedback was used to fine-tune the measurement instrument to ensure that the respondents understood the questions, were comfortable with the questions, and saw the questions as relevant. The feedback helped the researcher in structuring the flow of the questions. Bryman (2016) notes that pre-testing research measurement instruments is not only to do with ensuring the survey questions operate well but also ensures that the research instrument functions well.

3.7.1 Validity Tests

Bryman (2016) notes that research's validity measures the extent to which research design and the data that it yields allow the researcher to draw accurate conclusions. Internal validity addresses the integrity of the conclusions on the cause-effect relationship between variables thus determined by the research structure. External validity addresses the generalizability of the study's findings. Reliability is about how consistent or repeatable the study's results are (Bryman, 2016). To address validity, this study used standard analysis tools IBM SPSS and Microsoft Excel to perform

descriptive and inferential analysis that gave the correct relationship between the variables. The research measurement tool (questionnaire) went through a pilot study to ensure the respondents understood the questions, were comfortable with the questions, and saw the questions as relevant. The pilot study feedback helped the researcher to have the right flow of the questions

3.7.2 Reliability Tests

To ensure the reliability of the study, the questionnaire was administered only once to the respondents and the survey link was sent to the official email addresses of the respondents. Cronbach (1951) Alpha test was performed using IBM SPSS to test the internal consistency. Salkind (2007) recommends that for the measurement instrument to be reliable, it should have a minimum score of 0.7. The study conducted a pre-test of the research instruments and the analysis of the reliability metrics showed that resource factors had an Alpha score of 0.753, regulatory factors = 0.815, management support = 0.788, and cyber resilience = 0.755. Based on these scores the findings showed the study variables were within the acceptable range of internal consistency hence no further amendments were required in the research questionnaire.

3.8 Data Analysis and Presentation

Saunders et al. (2019) note that data analysis is about making conclusions on the relationships between the data variables that the research is designed to test to address the research questions and objectives. Saunders et al. note that some findings may be discovered that had not initially been planned for and hence, are still important to report on. Data analysis addressed the study's objectives which examined the impact of management support, resource factors, and regulatory factors on the overall cyber resilience within MFIs in Kenya. The responses were downloaded from Google forms while the physical copies were converted to excel format then data cleaning was done. Data analysis tools utilized by the study are IBM SPSS and Microsoft Excel. The study carried out several analyses: descriptive statistics, and inferential statistics. Diagrams such as frequency tables, pie charts, and bar graphs were used to present the data. According to Saunders et al. (2019), descriptive statistics describe and compare a variable's data values numerically and focus on two aspects of distribution: central tendency and dispersion. This study used the central tendency measures of mode, median, and mean to describe and compare data on management support, resource factors, and regulatory factors on the overall cyber resilience within MFIs in Kenya. The research further applied correlation analysis to establish the relation between the variables. Lastly, linear regression was done on all the variables and the coefficient of

determination (r^2) was obtained to determine the strength and direction of the relationship between the variables.

The linear regression analysis was based on Equation 3.1 below.

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon \qquad \text{Equation 3.1}$$

Where:

Y = cyber resilience in MFIs

X_1 = management support

X_2 = resource factors

X_3 = regulatory factors

β_1, β_2, and β_3 are regression coefficients of the independent variables

ε = variance errors component

α = inherent systems (cyber resilience without any cybersecurity investments)

3.9 Ethical Considerations

To ensure that the study meets ethical standards as set by the university policy and guidelines, the study used a university-stamped letter indicating the purpose and objective of the study. Respondents were asked for their consent orally before being issued the questionnaire. The purpose and nature of the study were informed to the respondents. Respondents' identities such as organization names, individuals' names, or contacts were not indicated in the questionnaire for confidentiality purposes. The online data collection tool Google Forms did not collect any system information such as the IP addresses of the respondents' computers. The study got approval from the National Commission for Science, Technology, and Innovation (NACOSTI) and Strathmore University allowing the researcher to access the identified respondents to obtain the necessary information for the study. The study emphasized the importance of confidentiality and indicated that the information gathered was specifically used for educational purposes only.

All research records will be stored in securely locked cabinets. That information may be transcribed into the Strathmore University database, but this will be sufficiently encrypted, and password protected. Only the people who are closely concerned with this study will have access

to anonymized information since respondents' organization names or contacts will not be captured in the questionnaire. The information will be kept confidential and used for academic purposes with the view of improving the cyber resilience posture in the financial sector. The information will not be used in any way without the respondents' express permission.

CHAPTER FOUR

PRESENTATION OF RESEARCH FINDINGS

4.1 Introduction

The research study was conducted across the registered wholesale, credit-only, and microfinance banks operating in Kenya. This chapter of the research presented the research findings derived from the analysis of the collected study data. The chapter was divided into the background information and the descriptive and inferential tests conducted based on the study objectives. Lastly, a summary of the study was provided at the end of the chapter.

4.2 Response Rate

The examination focused on the collection of research data from 50 CIOs/CISOs/IT Managers in the registered MFIs in operation within Kenya. The main approaches used in the data collection relied on physical questionnaires and Google forms as survey tools. The application of multiple approaches in the data collection was informed by the need for the study to maximize the response rate and ensure respondents have the freedom to respond using their desired approach. The study was able to obtain 49 responses representing a 98% response rate which was sufficient for use in the data analysis. The availability of the targeted participants was key to attaining the required information from all the institutions involved in the research.

4.3 Background Information

The section below provides information on the various demographic profile information sought from the various participants of the study.

Table 4.1 Summary of Demographic Information

Category			Frequency	Percent
Type of MFI		Credit-only MFI	34	69.0
		Wholesale MFI	2	4.0
		Microfinance Banks	13	27.0
		Total	49	100.0
Number of employees		1-9 employees	1	2.0
		10-49 employees	18	36.7
		50-99 employees	27	55.1
		100 and above	3	6.1
		Total	49	100.0
Annual Revenue of MFI		Less than 10 million	3	6.1
		11-20 million	17	34.7
		21-100 million	22	44.9
		Over 100 million	7	14.3
		Total	49	100.0
Role in the MFI institution		ICT Manager	29	59.0
		CISO’s	13	27.0
		CIO’s	5	14.0
		Total	49	100.0

The research focus was on the microfinance institutions operating in Kenya, and the findings revealed that the majority of the responses, 69% (n=34), were from credit-only institutions, 27% (n=13) were from microfinance banks, and only 4% (n=2) represented by wholesale microfinance firms in the country. The results were critical to the assessment of the factors affecting cyber resilience in the MFI industry, owing to the provision of responses from every registered firm in the country. The study was interested in the number of employees working within microfinance institutions, and the results pointed out that in the majority of the institutions, 55% (n= 27) had 50-99 employees, 37% (n= 18) had 10-49 employees, and only 2% of the firms had between 1-9 employees. The findings are an indication that microfinance institutions have an adequate workforce that can support the execution of cyber resilience practices in the industry.

The research examined the revenue generation capacity of the microfinance institutions, and the analysis is provided. The results show that most of the microfinance institutions 45% (n=22) had an annual turnover of 21-100 million, 35% (n=17) had an annual turnover of 11-20 million, 14% of the institutions generated a turnover of over 100 million, and 6% had an annual turnover of less than 10 million Kenya shillings. The analysis highlights that a majority of the institutions have adequate financial resources generation capacity which can be critical to enacting cyber resilience within the industry. The study results showed that most of the respondents, 59% of the respondents were ICT managers within the microfinance institutions, 27% were CISOs, and 14% were CIOs. The participants in the study play a central management role in the cyber and technology management within the institutions and are key to understanding how various factors impact cyber resilience in the industry.

4.4 Descriptive Analysis

The research sought to analyze the factors affecting cyber resilience in the microfinance industry in Kenya. The examination focussed on management support, resource factors, and regulatory factors. Descriptive analysis of the responses emanating from the Likert scale statements was conducted using mainly the standard deviation and the mean values. The findings are presented in this section in line with the variables of the research.

4.4.1 Management Support Factors

The study objective was to establish the effect of management support on the cyber resilience of microfinance institutions in Kenya. The analysis of the participants' responses is provided in Table

4.3 below. The following key was used in the interpretation; SA = strongly agree, A = agree, NA/ND = neither agree nor disagree, D = disagree, SD = strongly disagree

Table 4.2 Management Support Factors

	N	SD	D	NA/ND	A	SA	Mean	Std. Deviation
The management has put in place adequate internal ICT/cybersecurity policies which they monitor regularly.	49	40.8%	18.4%	24.5%	10.2%	6.1%	2.2245	1.26269
The organization management ensures there is a cybersecurity awareness programs that staff is mandated to take part in.	49	44.9%	18.4%	20.4%	16.3%	-	2.0816	1.15175
The organization has independent auditors who regularly assess the organization's cyber risks.	49	38.8%	28.6%	12.2%	18.4%	2%	2.1633	1.19630
The organization's management board has ICT competencies.	49	30.6%	24.5%	18.4%	18.4%	8.2%	2.4898	1.32480
The leadership team in our organization positively influence employees' attitude toward cyber security awareness.	49	36.7%	24.5%	24.5%	12.2%	2%	2.1837	1.13051
High training costs of the cybersecurity team impede internal capacity development	49	38.8%	18.4%	14.3%	18.4%	10.2%	2.4286	1.42887
The organization has in-house cybersecurity skills development programs to enhance staff cybersecurity skills.	49	44.9%	22.4%	16.3%	10.2%	6.1%	2.1020	1.26235
The top management ICT competency helps in determining the choice of technologies and tools that our organization adopts; and how these are in turn updated over time.	49	14.3%	2%	18.4%	32.7%	32.7%	3.6735	1.34455
The management has set up ICT structures with HR strategies that determine the quality of new entrants into the organization.	49	22.4%	20.4%	20.4%	26.5%	10.2%	2.8163	1.33344

The results show that participants agreed that top management ICT competency helps in determining the choice of technologies and tools that our organization adopts; and how these are in turn updated over time as noted by a mean of 3.6735. This result shows that the technical capacity of the management plays a major role in influencing IT governance and investment in technologies that support the enhancement of cyber resilience. This result showed that respondents were not in agreement on whether the management has set up ICT structures with HR strategies that determine the quality of new entrants into the organization (mean = 2.8163). This disagreement implies that several MFIs lack alignment between the ICT structure and the HR strategies for bringing employees onboard. The results show disagreement among respondents that the organization management ensures there are cybersecurity awareness programs that staff is

mandated to take part in (2.0816). This shows that the management in MFIs is to a large extent not influencing the cybersecurity awareness programs in their organizations. The analysis points to disagreement among respondents that the organization has in-house cybersecurity skills development programs to enhance staff cybersecurity skills (mean = 2.102). This result points to a shortage of cybersecurity skills in MFIs. Participants also disagreed on whether high training costs of the cybersecurity team impede internal capacity development as shown by a mean of 2.4286. This implies that apart from high training costs for cybersecurity, other factors are also impeding internal cybersecurity skills in MFIs.

4.4.2 Resource Factors

The second objective focused on how resource factors influence the cyber resilience of microfinance institutions in Kenya. The results from the various participants are summarized in Table 4.4 below. The following key was used in the interpretation; SA = strongly agree, A = agree, NA/ND = neither agree nor disagree, D = disagree, SD = strongly disagree

Table 4.3 Resource Factors

	N	SD	D	NA/ND	A	SA	Mean	Std. Deviation
The organization has adequate personnel with cybersecurity expertise	49	32.7%	20.4%	34.7%	8.2%	4.1%	2.3061	1.14025
High salary costs of the cybersecurity experts relative to other staff hinder the hiring of more cybersecurity experts	49	34.7%	30.6%	32.7%	-	2%	2.0408	.93450
There is a lack of skills to implement and support new cybersecurity technologies	49	28.6%	42.9%	22.4%	6.1%	-	2.0612	.87579
The organization does not have internal cybersecurity staff as we rely on cybersecurity solution vendor support which is sufficient	49	30.6%	28.6%	20.4%	12.2%	8.2%	2.3878	1.27175
Budget is a major constraint in the acquisition and implementation of new cybersecurity technologies	49	38.8%	22.4%	34.7%	2%	2%	2.0612	1.00847
The organization has in place good technical practices, good organizational practices, effective policies, and standards as drivers of cyber resilience	49	30.6%	24.5%	26.5%	12.2%	6.1%	2.3878	1.22162
The organization assess the cost of potential cybersecurity breaches to determine the right level of investment to mitigate the risk	49	38.8%	28.6%	18.4%	6.1%	8.2%	2.1633	1.24745
The organization's top management awareness about cyber attacks' success probability, influences higher investment in cyber resilience	49	10.2%	4.1%	18.4%	32.7%	34.7%	3.7755	1.26269

Respondents of the study agreed that the organization's top management awareness of cyber attacks' success probability, influences higher investment in cyber resilience as indicated by a mean of 3.7755. This indicates that resource allocation towards cyber resilience is influenced by how informed the management is on how vulnerable the organization is to cyber-attacks. The results show that respondents disagreed that the organization does not have internal cybersecurity staff as they rely on cybersecurity solution vendor support which is sufficient (mean = 2.3878). This means that MFIs largely rely on internal staff in executing their cybersecurity strategies. This point to a weakness in cybersecurity strategies since the MFIs have also indicated a lack of internal cybersecurity capacity building. The participants also disagreed with the statement that the organization assesses the cost of potential cybersecurity breaches to determine the right level of investment to mitigate the risk as noted by a mean of 2.1633. Cybersecurity investment by MFIs is not based on the anticipated cost of potential cybersecurity breaches. Findings revealed disagreement there is a lack of skills to implement and support new cybersecurity technologies as shown by a mean of 2.0612. Findings show the disagreement that the organization has adequate personnel with cybersecurity expertise as noted by 2.3061. This shows that MFIs have a shortage of cybersecurity experts.

4.4.3 Regulatory Factors

The third objective of the study focused on an analysis of the effect of regulatory factors on the cyber resilience of microfinance institutions in Kenya. The summary of the responses is shown below. The following key was used in the interpretation; SA = strongly agree, A = agree, NA/ND = neither agree nor disagree, D = disagree, SD = strongly disagree

Table 4.4 Regulatory Factors

	N	SD	D	NA/ND	A	SA	Mean	Std. Deviation
The organization has adopted and complies with financial industry cybersecurity regulations	49	6.1%	14.3%	22.4%	51%	6.1%	3.3673	1.01435
The organization participate in sharing cyber threats and intelligence with industry peers or government entities	49	4.1%	16.3%	14.3%	53.1%	12.2%	3.5306	1.04287
The lack of standards to guide the confidentiality and handling of the shared data hampers the organization's participation in information sharing	49	10.2%	42.9%	14.3%	20.4%	12.2%	2.8163	1.23615
Our organization has developed policies that guide access and use of private data.	49	10.2%	32.7%	20.4%	30.6%	6.1%	2.8980	1.14100
There are sufficient laws in tackling cybercrime and data privacy	49	2%	40.8%	28.6%	22.4%	6.1%	2.8980	.98414

The organization has in the past reported cybercrime matters to authorities, and the authorities fully addressed the matters	49	26.5%	40.8%	12.2%	12.2%	80.2%	2.3469	1.23408
The organization has a cyber insurance cover in place as a risk management measure	49	2%	16.3%	38.8%	34.7%	8.2%	3.3061	.91752
The cost of cybersecurity incidences is not clear to the organization hence, affecting the uptake of cyber insurance	49	6.1%	12.2%	38.8%	30.6%	12.2%	3.3061	1.04491
The extra cost associated with cyber information sharing impedes the organization's participation in information sharing	49	2%	14.3%	18.4%	51%	14.3%	3.6122	.97503

Participants agreed that the organization participates in sharing cyber threats and intelligence with industry peers or government entities, as indicated by a mean of 3.5306. The analysis showed agreement that the extra cost associated with cyber information sharing impedes the organization's participation in information sharing, as shown by a mean of 3.6122. The analysis showed no consensus among respondents on if the lack of standards to guide the confidentiality and handling of the shared data hampers the organization's participation in information sharing (mean = 2.8163). These results show that MFIs have embraced information sharing as a key component of their cyber resilience strategies. The respondents neither agreed nor disagreed on whether the cost of cybersecurity incidences is not clear to the organization hence, affecting the uptake of cyber insurance (mean = 3.3061). The results point to low uptake of cyber insurance by MFIs with only 2% of the respondents strongly agreeing. Further respondents did not agree on if the organization has in the past reported cybercrime matters to authorities and if the authorities fully addressed the matters (mean = 2.3469). Only 26.5% of the MFIs strongly agreed that past cybercrimes were addressed by authorities. This points to gaps in the addressing of cybercrimes.

4.4.4 Cyber Resilience in Microfinance Institutions

The study's dependent variable was focused on the analysis of the adoption of cyber resilience within microfinance institutions in Kenya, and the findings are shown below. The following key was used in the interpretation; SA = strongly agree, A = agree, NA/ND = neither agree nor disagree, D= disagree, SD = strongly disagree

Table 4.5 Cyber Resilience

	N	SD	D	NA/ND	A	SA	Mean	Std. Deviation
The organization has a documented cyber resilience strategy	49	36.7%	22.4%	18.4%	10.2%	10.2%	2.3878	1.39667
The organization regularly identifies and documents the cyber risks faced by the institution	49	28.6%	26.5%	20.4%	12.2%	12.2%	2.5306	1.35558
The organization classifies and prioritizes different cyber risks facing the institution	49	44.9%	12.2%	24.5%	8.2%	10.2%	2.2653	1.38106
The organization has set a baseline configuration to guide the setup of digital assets	49	38.8%	14.3%	16.3%	18.4%	12.2%	2.5102	1.47369
The organization ensures all threats and vulnerabilities identified are mitigated and documented	49	55.1%	14.3%	16.3%	12.2%	2%	1.9184	1.18738
The organization has implemented data confidentiality measures such as access control, network segmentation, and data encryption	49	34.7%	20.4%	28.6%	10.2%	6.1%	2.3265	1.23132
The organization has plans in place to ensure business operations continue in the event of an adverse scenario	49	30.6%	24.5%	18.4%	20.4%	6.1%	2.4694	1.29264
The organization periodically does drill tests on the business continuity plan to check its adequacy	49	14.3%	22.4%	24.5%	28.6%	10.2%	2.9796	1.23305
The organization has documented plans for responding to and aiding in recovering from cyber incidents that include recovery time objectives and recovery point objectives	49	14.3%	20.4%	32.7%	16.3%	16.3%	3.0000	1.27475

Findings show a lack of agreement among respondents on whether the organization has documented plans for responding to and aiding in recovering from cyber incidents that include recovery time objectives and recovery point objectives, as noted by a mean of 3.00. The respondents also did not agree or disagree on if the organization periodically does drill tests on the business continuity plan to check its adequacy (mean = 2.9796). The analysis show disagreement among respondents that the organization has plans in place to ensure business operations continue in the event of an adverse scenario (mean = 2.4694). These results show that only 30.6% of MFIs strongly agreed to have a business continuity plan in place. The analysis revealed disagreement among respondents on whether the organization has implemented data confidentiality measures such as access control, network segmentation, and data encryption (mean = 2.3265). This low score on implementing data confidentiality indicates that MFIs have gaps in implementing the data privacy laws and regulations that are in place in Kenya. The findings indicate disagreement that the organization ensures all threats and vulnerabilities identified are mitigated and documented

(mean = 1.9184). This lack of documentation on the threat landscape that MFIs are exposed to could leave the MFIs more vulnerable to similar threats hence reducing the cyber resilience within MFIs.

4.5 Correlation Analysis

The study focused on analyzing the effect of management support, regulatory factors, and resource factors on the cyber resilience of microfinance institutions. The research utilized the Spearman correlation approach, and the matrix is shown below.

Table 4.6 Correlation Matrix

			Cyber Resilience	Management Support	Regulatory Factors	Resource Factors
Spearman's rho	Cyber Resilience	Correlation Coefficient	1.000			
		Sig. (1-tailed)	.			
		N	49			
	Management Support	Correlation Coefficient	.366**	1.000		
		Sig. (1-tailed)	.005	.		
		N	49	49		
	Resource Factors	Correlation Coefficient	.417**	.057	.165	1.000
		Sig. (1-tailed)	.001	.348	.129	.
		N	49	49	49	49
	Regulatory Factors	Correlation Coefficient	.302*	.351**	1.000	
		Sig. (1-tailed)	.018	.007	.	
		N	49	49	49	

**. Correlation is significant at the 0.01 level (1-tailed).

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

The first objective analyzed the effect of management support on the cyber resilience of microfinance institutions. Results established there is a weak positive and significant effect of management support on the cyber resilience of microfinance institutions ($r = .366$, $sig = .005 < .05$). The second objective of the study sought to determine the effect of resource factors on the cyber resilience of microfinance institutions. Findings established there is a moderate positive and significant effect of resource factors on the cyber resilience of microfinance institutions ($r = .417$, $sig = .001 < .05$). The third objective focused on establishing the effect of regulatory factors on the cyber resilience of microfinance institutions. Analysis revealed there is a weak positive and

significant effect of regulatory factors on the cyber resilience of microfinance institutions (r = .302, sig = .018<.05).

4.6 Regression Analysis

The research conducted a regression analysis to examine how the various factors selected in the study influence the cyber resilience of microfinance institutions in Kenya. The study utilized the overall regression analysis to examine the joint effect of the independent variables. The overall regression testing focused on the joint effect of resource factors, regulatory factors, and management support on the cyber resilience in the microfinance institutions in Kenya.

Table 4.7 Overall Regression Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.583[a]	.339	.295	7.33583

a. Predictors: (Constant), Regulatory Factors, Resource Factors, Management Support

The above model showed that 33.9% of the changes in cyber resilience within microfinance institutions are predicted by the selected factors (management support, resource, and regulatory factors).

Table 4.8 Overall ANOVA Summary

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1243.984	3	414.661	7.705	.000[b]
	Residual	2421.649	45	53.814		
	Total	3665.633	48			

a. Dependent Variable: Cyber Resilience

b. Predictors: (Constant), Regulatory Factors, Resource Factors, Management Support

The ANOVA tests above yielded a F-value = 7.705, Sig = .000<.05. This implies there is a statistical significance between the three variables. The study thus showed there is a positive and statistically significant effect of management support, resource factors, and regulatory factors on the cyber resilience of MFIs.

Below are the coefficients yielded from the regression analysis:

Table 4.9 Overall Regression Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-2.424	7.801		-.311	.757
	Management Support	.406	.142	.371	2.859	.006
	Resource Factors	.633	.191	.411	3.310	.002
	Regulatory Factors	.124	.061	.060	2.033	.014

a. Dependent Variable: Cyber Resilience

$$Y = -2.424 + .406X_1 + .633X_2 + .124X_3 + 7.801$$

To establish the effect of management support on the cyber resilience of microfinance institutions in Kenya.

The findings showed a coefficient of management support that was significant ($.406X_1$, .006<.05) which revealed that changing management support will significantly contribute to an improvement in cyber resilience by a factor of .406.

To determine the influence of resource factors on the cyber resilience of microfinance institutions in Kenya.

The analysis showed a coefficient of resource factors that was significant ($.633X_2$, .002<.05) which revealed that changing resource factors will significantly contribute to an improvement in cyber resilience by a factor of .633.

To evaluate the effect of regulatory factors on the cyber resilience of microfinance institutions in Kenya.

The findings showed a coefficient of regulatory factors that was significant ($.124X_3$, .014<.05) which revealed that changing regulatory factors will significantly contribute to an improvement in cyber resilience by a factor of .124.

4.7 Chapter Summary

The fourth chapter focused on a presentation of the research findings, which revealed the examination was able to obtain a 98% response rate. 59% of the research responses were obtained from the ICT managers of the MFIs thus underpinning the relevancy of the information provided in analysing how various factors influence cyber resilience. The study revealed that most of the

participants 55% had at least 50-99 employees. The correlation analysis showed that management support, resource factors, and regulatory factors positively influenced the cyber resilience of microfinance institutions. The regression established that at least 33.9% of the changes in cyber resilience within microfinance institutions are determined by management support, resource factors, and regulatory factors.

CHAPTER FIVE

DISCUSSION, CONCLUSION, AND RECOMMENDATION

5.1 Introduction

This is the final chapter of the study. It presents a discussion of the study findings and the conclusions that were drawn. The section will present the research findings in line with the study objectives. After presenting the findings, the chapter will present the recommendations that can be drawn and the recommendations for future research based on the gaps identified.

5.2 Discussion

This section presents a discussion of the study findings presented in line with the study objectives and backed by empirical evidence. The analysis concluded that there is a strong positive relationship between regulatory factors, resource factors, management support, and cyber resilience of microfinance institutions in Kenya. These findings support the premise of the RBV theory, which opines that through the application of their internal capabilities, resource pool, and key competencies organizations can be able to achieve some competitiveness in the industry. From the results, there is evidence that an organization that can effectively manage its resources, harness the management support, and ensures they review the regulatory environment can be able to improve the organization's cyber resilience. Similarly, as underlined in the game theory, the ability of the organization management to support change policies and processes to meet regulatory recommendations and compliance requirements formulated will promote industry-wide cyber resilience. This is supported by the results that have shown a significant and positive effect of management support, resource factors, and regulatory factors on the adoption of cyber resilience within the MFI industry.

5.2.1 Management Support and Cyber Resilience

The first objective sought the effect of management support on the cyber-resilience of MFIs in Kenya. The analysis determined that the support of the top management has a significant positive effect on organizations' cyber-resilience. This is in accordance with the RBV theory which avers that firms with leaders who have a clear understanding of cyber threats will support their organizations towards becoming cyber resilient. The analysis revealed that resource allocation towards cyber resilience is influenced by how informed the management is on the vulnerability of the organization to cyber-attacks. This is in line with the Game theory which provides a means or

strategies for managers to allocate resources in the ever-changing cyberspace, including the managers' support in implementing strategies aimed at ensuring microfinance firms become cyber-resilience.

The study revealed that changing management support significantly contributes to an improvement in cyber resilience by a factor of .406. These findings collaborated in the study by Lykou et al. (2019), which ascertained that managers play a key role in developing a structural and procedural basis that can enhance continuous intra-and inter-organizational cyber resilience analysis, managing interdisciplinary cyber-risk analysis teams, developing and maintaining a portfolio of cyber-threat scenarios, and creating consistency and synergy in safety and security. Similarly, Jensen (2015) studied cyber resilience in the maritime industry and determined that maritime managers are essential in developing a set of best practices and guidelines that can direct cyber-resilience and orient long-term goals with global cybersecurity standards.

In Ghana, Affum (2019) investigated organizational cyber resilience in foreign banks and ascertained that managerial support is essential to creating communication systems. The research determined that the ability to maintain voice and data communication always is critical to facilitating threat assessment and response. The study showed that communication improves coordination capability, which influences the level of cooperation between a wide range of security agencies and facilitates cyber-resilience. Furthermore, according to Hausken (2020), managers are essential determinants of microfinance firms' ability to predict and analyse future threats. The analysis showed that the management's commitment to cyber resilience could be determined by the number of resources allocated towards ensuring organizational cyber resilience.

Matern et al. (2019) studied the role of managers in facilitating cyber resilience in public administration and reported similar findings, showing that managers play a key role in selecting human resource strategies that direct recruitment, set corporate ICT structure, and determine the degree to which employees receive infrastructural and cultural support. Top leadership support was determined to be the driving force behind institutional change and increased awareness regarding good cyber resilience practices, and instituting changes to address the retention of employees with the required skills. Balakrishnan et al. (2018) found that managers shape cyber resilience strategies and can influence monitoring and detection procedures, cyber resilience culture, communication and coordination, and recovery planning. However, the researchers

determined that the managers' aversiveness towards risk influences the organizational approach towards cyber-resilience.

5.2.2 Resource Factors and Cyber Resilience

The second objective of the study was to determine the relationship between resource factors and cyber-resilience. The analysis showed that resource factors have a significant effect on cyber-resilience within microfinance institutions in Kenya. This is in accordance with the RBV theory which avers that the resources accrued by an organization affect the degree of investment and execution of cybersecurity practices within the organization. Game theory provides a means for analysing the continuous defense measures to be employed and directing the investments to the most impactful defense measures. The study revealed that changing resource factors significantly contribute to an improvement in cyber resilience by a factor of .633. These sentiments were also reported in the study by Catota et al. (2018), which found evidence that the quality of resources under control by an organization has a significant influence on the degree of a firm's cyber-resilience. Similarly, Carías et al. (2019) study sought expert opinion and ascertained that the skills and competencies of the cyber security team, the degree of investment in technologies, and the frequency of cybersecurity training influence how secure firms will be. The study ascertained that managers must allocate adequate financial resources to gain the technical capacity necessary to guarantee cyber resilience.

These findings were also reported by Lykou, Anagnostopoulou, et al. (2019), who researched threat mitigation and cyber resilience controls in smart airports and determined that good technical practices, good organizational practices, and effective policies and standards are among the main drivers of organizational cyber resilience. The study by Annarelli & Palombi (2021) also found that firms that possess a unique set of heterogeneous and diversified resources and are supported by competent leadership are in a better position to reconfigure these resources to address cyber resilience challenges. In the study by Kasanga (2021), organizational recruitment strategies determine the technical capacity of an organization's workforce, which is essential to facilitating continuous learning and innovation, effective deployment of heterogeneous resources, and enhanced cyber resilience.

According to the study by Kumar et al. (2021), the type of technologies used by an organization determines its level of cyber resilience. The degree of adoption can be accelerated by the degree of enforcement of legal consequences upon non-compliance to regulations. The study also showed

positive relationships between adherence to information security standards and organizational resilience and cyber resilience. Akech et al. (2020) studied cyber resilience factors within county governments in Kenya and showed that the technical competence of IT staff, financial resources allocated towards cyber security, compliance requirements, and management support were all antecedents of cyber resilience. Long-term resilience is guaranteed by an organization's access to qualified IT technical cyber security specialists who can make industry assessments and formulate effective cyber resilience strategies.

5.2.3 Regulatory Factors and Cyber Resilience

The third objective of the study was to examine the effect of regulatory factors on the cyber resilience of microfinance institutions in Kenya. The analysis showed the positive and significant effect of regulatory factors on the cyber resilience of microfinance institutions. Regulations are also enablers of cyber resilience. The RBV theory identifies regulations as resources that firms can utilize in the development of cyber security frameworks. Firms with competent managers, who invest in cyber security technologies and skilled cyber security, according to the RBV will be more competitive and able to become cyber resilient. The Game theory was useful in explaining how organizations change policies and processes in response to the cyber security environment.

The study revealed that changing regulatory factors contribute to an improvement in cyber resilience by a factor of .124. The analysis revealed that regulations are key to providing direction on legal and cyber security frameworks that would direct firms' approaches to meet cyber resilience.

These findings were reported in the literature review by Bagheri and Ridley (2017), which found evidence that instituting regulatory frameworks is one way to guide firms by providing a checklist for minimum cyber resilience requirements that boards are required to implement. The study also showed that establishing audit requirements as internal risk assessment measures enhances risk detection, response, and reporting, which has a positive correlation with cyber resilience. Similar findings were reported by Mughairi et al. (2019), who determined that establishing legal requirements for critical service providers to have local security divisions dedicated to upholding the integrity of their systems would have a significant positive effect on the national systems' cyber resilience. The study also determined that aligning cybersecurity governance frameworks with organization-wide governance processes and procedures would improve the effectiveness of cyber resilience. Adu & Adjei (2018) also showed a positive impact of regulatory policies and cyber

resilience, arguing that cyber resilience knowledge and awareness alone are not guarantees of effective implementation of cyber resilience structures within corporate institutions.

The study also showed a failure to enforce information security standards had harmed financial institutions' cyber resilience. The researchers called for greater enforcement of legally recommended standards and information security practices as a means of strengthening overall organizational resilience. The study by Karabacak et al. (2020) showed that having clearly defined and communicated governance mechanisms would improve cyber resilience among firms in the space industry. The study determined that documenting cyber resilience commitments, strategies, principles, policies, rules, and procedures would provide an adequate governance framework that would guide cyber resilience. The study reported that the existing framework does not provide cover for all types of digital products, impacting cyber resilience. Karabacak & Tatar (2017) averred that cyber maturity can be determined by the quality of regulatory guidelines and that a national cybersecurity program would facilitate the implementation of cooperation and collaboration routines and information exchange strategies and strengthen the legal foundations. These studies provide supporting evidence that having well-defined and enforced regulations would improve a firm's decisions to implement concrete resilience strategies that would improve its resilience metrics. Adhering to regulatory requirements and international resilience practices has been guaranteed to improve a firm's cyber resilience.

5.3 Conclusions

The analysis pointed out that the three selected variables; management support, resource factors, and regulatory factors, are critical to the implementation of cyber resilience in microfinance institutions in Kenya. This aligns with the main tenets of the Resource Based View theory which affirms that a firm's resources have a significant impact on its ability to realize organizational goals, in this case becoming cyber resilient. Managerial knowledge and support of cyber resilience, the employees' technical competencies, and the level of regulatory development are all factors that can be attributed to RBV as significant determinants of a firm's ability to withstand and recover from cyber-attacks. Game theory provides means or strategies for managers to analyse the continuous defense measures to be employed and direct investments to the most impactful defense measures. The Game theory was also useful in explaining how organizations change and adapt policies and processes such as information sharing in response to the cyber security environment to attain cyber resilience.

Regarding the first objective, the study concludes that there is a significant positive relationship between management support and microfinance firms' cyber resilience. Managers were reported to influence cyber resilience in a variety of ways, such as cultivating cyber security interest, providing employee empowerment, allocating cyber security budget, and commissioning good cyber resilience practices. This implies that it would be paramount for organizations seeking to attain the cyber resilience status to hire managers who are conscious of cyber threats to ensure that they provide competent technical and financial support and redirect organizational efforts towards meeting cyber resilience requirements. The study also determined that managers have an important role to play when it comes to internal coordination and the creation of cyber resilience programs. They are also instrumental when it comes to the selection and empowering of cyber resilience teams and internal and independent auditors who were determined to improve risk detection and reporting.

From the analysis, conclusions were that resource factors have a significant positive effect on organizational cyber resilience, implying that organizations are more cyber resilient if they can acquire and retain adequate and competent IT professionals who are knowledgeable of the risks threatening organizational performance. The research determined that microfinance organizations must direct sufficient financial resources towards meeting the cyber resilience team's budgetary demands as budgetary constraints were affirmed to have an impact on the effective implementation of cyber security solutions. The study also determined that the quality of technological infrastructure that already exists in the organization has a significant impact on an organization's ability to successfully integrate emerging cyber technologies into the security setup and meet cyber resilience goals.

The study also concluded that regulatory factors have a significant impact on an organization's cyber resilience, implying that having effective policies and standard requirements in place would improve the organization's intentions to comply and hence attain cyber resilience. The study conclusions showed that adopting and complying with financial industry cyber security regulations, participating in cyber threat and intelligence briefing with industry peers, and developing policies that guide data privacy would improve a firm's cyber resilience. The study also showed that having sufficient laws tackling cybercrime and addressing cyber incidence reporting would improve a firm's intention to comply with the requirements established and

participate in information sharing. Therefore, firms that follow strict codes of conduct, participate in threat disclosure, and ascribe to ethical practices are guaranteed to meet cyber resilience status.

5.4 Recommendations

The research sought to determine the factors that influence cyber resilience within microfinance firms and determined that management support, resource, and regulatory factors all have significant effects on the institution's cyber resilience. The degree of management support, the quality of resources available, and the degree of compliance with industry regulations determine how secure the organizations will be from cyber threats. The study recommends that to be more cyber resilient, the firms must be ready to allocate significant resources, both financial and technical to ensure that they meet the high costs associated with pursuing cyber resilience status. Significant investments must be made to acquire the technologies and competence necessary to ensure they meet internationally recognized cyber resilience standards.

The study also recommends that managements take a central role in promoting the institution's cyber resilience. Managers should be directly involved in formulating cyber resilience strategies, selecting cyber resilience programs, and allocating resources that would enable firms to become more cyber resilient. The study also recommends that managers align security decisions with organizational goals and capabilities to reduce organizational misalignment, which can affect effective cyber resilience implementation.

The study established that coordinated approaches have a direct positive impact on cyber resilience and recommend that microfinance firms utilize multiple channels of information sharing and communication to raise the level of knowledge and attention directed towards meeting cyber resilience and improving threat detection, assessment, and mitigation. The study also concluded that regulatory factors have a significant effect on cyber resilience within microfinance institutions, and recommendations are that policymakers align with industry players to assess the industry's readiness and to develop a set of standards and regulations that all firms are capable of meeting as this would promote cyber resilience.

5.5 Suggestions for Further Research

This study focused on investigating cyber resilience within microfinance firms in Kenya. Based on the available literature, this study found minimal exploration of cyber resilience across various industries. This study recommends exploration into cyber resilience in non-financial industries such as the healthcare and manufacturing sectors which are highly reliant on information security

for effectiveness. Further research should also be carried out to determine the impact of the regulatory framework on cyber resilience, as this would provide a more in-depth understanding of the importance of regulation in facilitating cyber industry resilience. This study's respondents were ICT staff hence, future research on cyber resilience should also incorporate the end-users who are the non-ICT staff to understand their contribution to a firm's cyber resilience.

5.6 Limitations of the Study

This study was limited to investigating cyber resilience practices within microfinance firms. The study limited itself to collecting primary data from security and IT managers. The study also limited itself to the Resource Based View and the Game Theory in explaining the determinant factors of cyber resilience within microfinance firms. Further, the research was only focused on MFI institutions hence more in-depth research can be conducted focusing on the overall financial sector in Kenya.

References

Abraham, C., & Sims, R. R. (2021). A Comprehensive Approach to Cyber Resilience. *MIT Sloan Management Review62(3), 1-4.*, 62(3), 1-4.

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*, 20, (2).

Affum, C. (2019). Cybersecurity Practices among Foreign Banks in Ghana. *Doctoral dissertation, University of Ghana*.

Ahmed, R., & Philbin, S. P. (2022). Impact of senior management support on leadership competencies and the success of social sector projects in Pakistan. *Project Leadership and Society*.

Akech, P., Abeka, S., & Liyala, S. (2020). A Framework Based On Institutional Theory To Aid In Cyber Resiliency In County Governments Of Kenya. *International Journal of Innovative Research and Advanced Studies (IJIRAS)*, 7 (7), 142-147.

Al Mughairi, B. M., Al Hajri, H. H., Karim, A. M., & Hossain, M. I. (2019). An innovative cyber security based approach for national infrastructure resiliency for Sultanate of Oman. *International Journal of Academic Research in Business and Social Sciences*, 9(3), 1180-1195.

Alina, C. M., Cerasela, S. E., & Gabriela, G. (2017). Internal audit role in cybersecurity. *Ovidius University Annals: Economic Sciences Series*, 17(2), 510-513.

Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability*, 13(23), 13065.

Apanja, B., & Matabi, M. (2021). Cybersecurity readiness of SACCOs in Kenya . *KUSSCO*.

Bagheri, S. (2020). Investigating organisational aspects of cyber resilience in large organisation. *Doctoral dissertation, University of Tasmania*.

Bagheri, S., & Ridley, G. (2017). Organisational cyber resilience: research opportunities. *ACIS2017: Australasian Conference on Information Systems*, (pp. 1-10).

Balakrishnan, U. R., Mishra, G., & Bhatt, N. (2018). *Strategies for Improving Cyber Resilience of Data-Intensive Business Information Systems.* Auerbach Publications.

Barham, H., Dabic, M., Daim, T., & Shifrer, D. (2020). The role of management support for the implementation of open innovation practices in firms. *Technology in Society*, 63, 101282.

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an industrial internet of things context. *Sensors*, 19(1), 138.

Chatzoglou, P., Chatzoudes, D., Sarigiannidis, L., & Theriou, G. (2018). The role of firm-specific factors in the strategy-performance relationship: Revisiting the resource-based view of the firm and the VRIO framework. *Management Research Review*.

Chizanga, M. K., Agola, J., & Rodrigues, A. (2022). Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities. *International Research Journal of Innovations in Engineering and Technology*, 6(1), 54.

Chumphong, O., Srimai, S., & Potipiroon, W. (2020). The Resource-Based View, Dynamic Capabilities and SME Performance for SMEs to Become Smart Enterprises. *ABAC ODI Journal Vision. Action. Outcome*, 7(2), 129.

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

CSIS. (2022). *Center for Strategic and International Studies*. Retrieved from www.csis.org: https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/financial-sector-cybersecurity#:~:text=Financial%20institutions%20are%20leading%20targets,for%20political%20and%20ideological%20leverage.

Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). *Cyber risk definition and classification for financial risk management.* Federal Reserve Bank of St Louis.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations? *International Journal of Business & Society*, 19(1).

Diin Fitri, S. E., Dahlan, R. M., & Sukardi, S. (2018). From Penrose to Sirmon: The evolution of resource based theory. *Journal of Management and leadership*, 1(2).

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

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8(1), 1-26.

Felton Jr, J. H. (2021). Cyber Resilience of Small Business Owners. *Doctoral dissertation, Capella University*.

Ferdinando, L. (2016). Doctoral dissertation, Georgetown University. *Cybersecurity: How Safe Are We As A Nation?*

Freeman, R. E., Dmytriyev, S. D., & Phillips, R. A. (2021). Stakeholder theory and the resource-based view of the firm. *Journal of Management*, 47(7), 1757-1770.

Ghapanchi, A. H., Wohlin, C., & Aurum, A. (2014). Resources contributing to gaining competitive advantage for open source software projects: An application of resource-based theory. *International Journal of Project Management*, 32(1), 139-152.

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

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science*, 679(1), 140-157.

Hsu, H. Y., Liu, F. H., Tsou, H. T., & Chen, L. J. (2019). Openness of technology adoption, top management support and service innovation: a social innovation perspective. *Journal of Business & Industrial Marketing*.

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences.*

Jensen, L. (2015). Challenges in maritime cyber-resilience. *Technology Innovation Management Review*, 5(4), 35.

Karabacak, B., & Tatar, U. (2017). *From the National Cyber Maturity to the Cyber Resilience: The Lessons Learnt from the Efforts of Turkey.* Franklin University Scholarly Exchange.

Karabacak, B., Ikitemur, G., & Igonor, A. (2020). A Mixed Public-Private Partnership Approach for Cyber Resilience of Space Technologies. *Franklin University*.

Kasanga, J. N. (2021). Outcome of Techniques Employed for Cyber Resiliency by Commercial Banks in Kenya. *Doctoral dissertation, University of Nairobi*.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, (8), 11-14.

Kigen, M. P., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., . . . Shitanda, S. (2015). *Kenya Cyber Security Report 2015.*

Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. *arXiv preprint arXiv:2102.09455.*

Kovanen, T., Nuojua, V., & Lehto, M. (2018). Cyber threat landscape in energy sector. *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 353). Academic Conferences and publishing limited.

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, 34 (6), 1597-1629.

Laban, A. M. (2021). Digital Economy and Cybercrime. *great expectations: defining a trans-mediterranean cybersecurity agenda*, 16.

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business horizons*, 61(1), 35-46.

Linkov, I., & Kott, A. (2019). *Fundamental concepts of cyber resilience: Introduction and overview*. Cyber resilience of systems and networks.

Lo, M. F., Tian, F., & Ng, P. M. (2021). Top management support and knowledge sharing: the strategic role of affiliation and trust in academic environment. *Journal of Knowledge Management*.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, 19(1), 19.

Lykou, G., Iakovakis, G., & Gritzalis, D. (2019). Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management. *Critical Infrastructure Security and Resilience*, 245-260.

Mandal, S. (2020). Impact of supplier innovativeness, top management support and strategic sourcing on supply chain resilience. *International Journal of Productivity and Performance Management*.

Matern, S., Savova, G., Goleva, D., & Shalamanov, V. (2019). Human Factor in Digitalization and Cyber Resilience of Public Administration. *Computer and Communications Engineering*, 13(2), 3-15.

Matern, S., Savova, G., Goleva, D., & Shalamanov, V. (2019). Human Factor in Digitalization and Cyber Resilience of Public Administration. *Computer and Communications Engineering*, 13(2), 3-15.

Miller, D. (2019). The resource-based view of the firm. *Oxford Research Encyclopedia of Business and Management*.

Minnaar, A. &. (2021). Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, 34(3), 155-185.

Muhati, E. (2018). Factors affecting cyber-security in Kenya – A Case of Small Medium. *Strathmore Business School (SBS)*.

Muraguri, N. N., Mwalili, T., & Mose, T. (2019). Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County. *International Academic Journal of Information Systems and Technology*, 2(1), 157.

Nallainathan, S. (2021). Analysis onto the Evolving Cyber-Attack Trends during COVID-19 Pandemic. *International Journal of Science and Research (IJSR)*, 10(4).

Nandi, M. L., Nandi, S., Moya, H., & Kaynak, H. (2020). Blockchain technology-enabled supply chain systems and supply chain performance: a resource-based view. Supply Chain Management. *An International Journal*.

North, J., & Pascoe, R. (2016). Cyber security and resilience It's all about governance. *Governance Directions*, 68(3), 146-151.

Nyesemane, T. E. (2021). A Framework for Top Management Support Practices for the Successful Delivery of Projects in Revenue Administrations in SACU. *Doctoral dissertation, North-West University (South Africa)*.

Orji, U. J. (2019). An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. *Computer Law & Security Review*, 35(6), 105330.

Putranti, I. R., Windiani, R., Farabi, N., Amaliyah, A., & Rosyidin, M. (2020). Cyber Resilience of Small and Medium Enterprises in Semarang City. *MIMBAR: Jurnal Sosial dan Pembangunan*, 36(2), 288-297.

Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M. V., Lambert, J. H., . . . Todorovic, B. (2017). Bridging the gap from cyber security to resilience. *Resilience and Risk*, 383-414.

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, 39(1), 1-19.

Soikkeli, J., Casale, G., Munoz-Gonzalez, L., & Lupu, E. C. (2022). Redundancy Planning for Cost Efficient Resilience to Cyber Attacks. *IEEE Transactions on Dependable and Secure Computing*.

Solesvik, M. (2018). The rise and fall of the resource-based view: paradigm shift in strategic management. *Journal of new economy*, 19(4), 5-18.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178-188.

Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. *Cybersecurity Governance*, 37-56.

Tohănean, D., Buzatu, A. I., Baba, C. A., & Georgescu, B. (2020). Business model innovation through the use of digital technologies: Managing risks and creating sustainability. *Amfiteatru Economic*, 22(55), 758-774.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387.

Van de Mark, R. (2020). Industry of Anonymity: Inside the Business of Cybercrime, by Jonathan Lusthaus. *Osgoode Hall Law Journal*, 56(3), 683-688.

Whitfield, K. (2019). *The Resource-Based View approach and HRM. In Elgar Introduction to Theories of Human Resources and Employment Relations.* Edward Elgar Publishing.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, 16(4), 490-513.

Zwikael, O., & Meredith, J. R. (2019). The role of organizational climate in setting project goals. *International journal of operations & production management*.

APPENDICES

Appendix I: Letter of Introduction to Microfinance Institutions

Ole Sangale Rd, Madaraka Estate,
P.O Box 59857 00200, Nairobi, Kenya.
Cell: +254 703 414/6/7, Twitter: @SBSKenya
Email: info@sbs.ac.ke or visit **www.sbs.strathmore.edu**

Strathmore UNIVERSITY
BUSINESS SCHOOL

Friday, 18th March 2022

To Whom It May Concern,

RE: FACILITATION OF RESEARCH – MOSES EDEMBA KIGANDA

This is to introduce Moses Edemba Kiganda who is a **Master of Business Administration** (MBA) student at Strathmore University Business School, admission number MBA 136365. As part of our MBA Program, Moses is expected to do applied research and undertake a project. This is in partial fulfilment of the requirements of the MBA course. To this effect, he would like to request for appropriate data from your organization.

Moses is undertaking a research paper on **"An Assessment of The Factors Affecting Cyber Resilience in Microfinance Institutions in Kenya."** The information obtained from your organization shall be treated confidentially and shall be used for academic purposes only.

Our MBA Program seeks to establish links with industry, and one of these ways is by directing our research to areas that would be of direct use to industry. We would be glad to share our findings with you after the research, and we trust that you will find them of great interest and of practical value to your organization.

We appreciate your support and shall be willing to provide any further information if required.

Yours Faithfully,

Caroline Tiara.
Manager – Graduate Programs.
Strathmore University Business School

Appendix II: Research Questionnaire

Instructions: Answer the questions by ticking the appropriate choice in the checkbox.

Section 1: Background Information

1. What is the category of your institution?
   - ☐ Microfinance Bank
   - ☐ Credit Only Microfinance Institution
   - ☐ Wholesale Microfinance Institution
2. How many employees does your organization have?
   - ☐ 1 - 9
   - ☐ 10 – 49
   - ☐ 50 – 99
   - ☐ 100 and above
3. What is the approximate annual business revenue turnover in Kenya Shillings?
   - ☐ Less than 10 million
   - ☐ 11 – 20 million
   - ☐ 21 – 100 million
   - ☐ Above 100 million
4. What is your job role in the institution?
   - ☐ Chief Information Officer (CIO)
   - ☐ Chief Information Security Officer (CISO)
   - ☐ ICT Manager/Director
5. Select the activities that are part of your job role
   - ☐ Establishing the cybersecurity strategy and governance
   - ☐ Allocation of budget to cybersecurity
   - ☐ Structuring ICT personnel
   - ☐ Ensuring organization compliance to cybersecurity measures
   - ☐ Securing the organization's ICT systems
   - ☐ Determining technology investments by the organization
   - ☐ Enforcement of industry cybersecurity regulations

☐ Taking part financial industry cybersecurity collaborations

☐ Approving cybersecurity training for employees

PART B: ANALYSIS OF THE FACTORS THAT INFLUENCE THE CYBER RESILIENCE OF MICROFINANCE INSTITUTIONS IN KENYA

Please indicate in the table with a tick (√) your level of agreement based on the below scale:

1= Strongly Disagree 2= Disagree 3= Neither Agree nor Disagree 4= Agree

5= Strongly Agree

No	Management Support	1	2	3	4	5
(1.)	The management has put in place adequate internal ICT/cybersecurity policies which they monitor regularly.					
(2.)	The organization management ensures there is a cybersecurity awareness programs that staff are mandated to take part in.					
(3.)	The organization has independent auditors who regularly assess the organization cyber risks.					
(4.)	The organization's management board has ICT competencies.					
(5.)	The leadership team in our organization positively influence employees' attitude towards cyber security awareness.					
(6.)	High training costs of the cybersecurity team impede internal capacity development					
(7.)	The organization has in-house cybersecurity skills development programs to enhance staff cybersecurity skills.					
(8.)	The top management ICT competency helps in determining the choice of technologies and tools that					

	our organization adopts; and how these are in turn updated over time.					
(9.)	The management has set up ICT structures with HR strategies that determine the quality of new entrants into the organization.					

No	**Resource factors**	**1**	**2**	**3**	**4**	**5**
(1.)	The organization has adequate personnel with cybersecurity expertise					
(2.)	High salary costs of the cybersecurity experts relative to other staff hinder the hiring of more cybersecurity experts					
(3.)	There is a lack of skills to implement and support new cybersecurity technologies					
(4.)	The organization does not have internal cybersecurity staff as we rely on cybersecurity solution vendor support which is sufficient					
(5.)	Budget is a major constraint in the acquisition and implementation of new cybersecurity technologies					
(6.)	The organization has in place good technical practices, good organizational practices, effective policies, and standards as drivers of cyber resilience.					
(7.)	The organization assess the cost of potential cybersecurity breaches to determine the right level of investment to mitigate the risk					
(8.)	The organization's top management awareness about cyber attacks' success probability, influences higher investment in cyber resilience.					

No	Regulatory factors	1	2	3	4	5
(1.)	The organization has adopted and complies with financial industry cybersecurity regulations					
(2.)	The organization participate in sharing cyber threats and intelligence with industry peers or government entities					
(3.)	The lack of standards to guide the confidentiality and handling of the shared data hampers the organization's participation in information sharing					
(4.)	Our organization has developed policies that guide access and use of private data.					
(5.)	There are sufficient laws in tackling cybercrime and data privacy					
(6.)	The organization has in the past reported cybercrime matters to authorities and the authorities fully addressed the matters					
(7.)	The organization has a cyber insurance cover in place as a risk management measure					
(8.)	The cost of cybersecurity incidences is not clear to the organization hence, affecting uptake of cyber insurance					
(9.)	The extra cost associated with cyber information sharing impedes the organization's participation in information sharing.					

PART C: CYBER RESILIENCE OF MICROFINANCE INSTITUTIONS IN KENYA

Please indicate in the table with a tick (√) your level of agreement based on the below scale:

1= Strongly Disagree 2= Disagree 3= Neither Agree nor Disagree 4= Agree

5= Strongly Agree

No	Cyber resilience	1	2	3	4	5

(1.)	The organization has a documented cyber resilience strategy					
(2.)	The organization regularly identifies and documents the cyber risks faced by the institution					
(3.)	The organization classifies and prioritizes different cyber risks facing the institution					
(4.)	The organization has set a baseline configuration to guide the setup of digital assets					
(5.)	The organization ensures all threats and vulnerabilities identified are mitigated and documented					
(6.)	The organization has implemented data confidentiality measures such as access control, network segmentation, and data encryption					
(7.)	The organization has plans in place to ensure business operations continue in the event of an adverse scenario					
(8.)	The organization periodically does drill tests on the business continuity plan to check its adequacy					
(9.)	The organization has documented plans for responding to and aid in recovering from cyber incidents that include recovery time objectives and recovery point objectives					

Thank you for participating in the research.

Appendix III: Population of MFIs for the Study (Source: (AMFI-K, 2020; CBK, 2020))

Research Code Number	Name of MFI	MFI Category	Location	Website
1	Faulu Microfinance Bank Ltd	Microfinance Bank	Nairobi County	https://www.faulukenya.com/
2	Kenya Women Microfinance Bank	Microfinance Bank	Nairobi County	https://kwftbank.com/
3	Rafiki Microfinance Bank	Microfinance Bank	Nairobi County	https://www.rafikibank.co.ke/
4	SMEP Microfinance Bank Ltd	Microfinance Bank	Nairobi County	https://www.smep.co.ke/
5	Maisha Microfinance Bank	Microfinance Bank	Nairobi County	https://maishabank.com/
6	Caritas Microfinance Bank	Microfinance Bank	Nairobi County	https://caritas-mfb.co.ke/
7	Sumac Microfinance Bank	Microfinance Bank	Nairobi County	https://sumacmicrofinancebank.co.ke/
8	U&I Microfinance Bank	Microfinance Bank	Nairobi County	https://www.uni-microfinance.co.ke/
9	Key Microfinance Bank Ltd	Microfinance Bank	Nairobi County	https://keymicrofinancebank.com/
10	Uwezo Microfinance Bank	Microfinance Bank	Nairobi County	https://www.uwezomfbank.com/
11	Century Microfinance Bank	Microfinance Bank	Nairobi County	https://century.co.ke/
12	Daraja Microfinance Bank	Microfinance Bank	Nairobi County	https://darajabank.co.ke/
13	Choice Microfinance Bank	Microfinance Bank	Ongata Rongai	https://www.choicemfb.com/
14	Muungano Microfinance Bank	Microfinance Bank	Muranga County	https://muunganomfbank.co.ke/
15	ECLOF Kenya	Credit-Only MFI	Nairobi County	https://www.eclof-kenya.org/
16	Vision Fund Kenya Limited	Credit-Only MFI	Nairobi County	https://visionfundkenya.co.ke/
17	BIMAS Kenya Ltd	Credit-Only MFI	Embu County	https://www.bimaskenya.com/
18	Letshego Kenya Ltd	Credit-Only MFI	Nairobi County	https://www.letshego.com/kenya
19	Zenka Finance Ltd	Credit-Only MFI	Nairobi County	https://zenka.co.ke/
20	YEHU Microfinance Trust	Credit-Only MFI	Mombasa County	https://www.yehu.org/
21	Jitegemea Credit Scheme	Credit-Only MFI	Nairobi County	https://www.jitegemea.co.ke/
22	Fincredit Services Ltd	Credit-Only MFI	Nairobi County	https://fincredit.co.ke/
23	Juhudi Kilimo Co.Ltd	Credit-Only MFI	Nairobi County	https://juhudikilimo.com/
24	Musoni Kenya Ltd	Credit-Only MFI	Nairobi County	https://musoni.co.ke/
25	Select Management Services Ltd	Credit-Only MFI	Nairobi County	https://www.selectafrica.net/kenya/
26	Greenland Fedha Ltd	Credit-Only MFI	Nairobi County	http://gfedha.com/
27	Platinum Credit Limited	Credit-Only MFI	Nairobi County	https://platinumcredit.co.ke/
28	Habitat for Humanity International	Credit-Only MFI	Nairobi County	https://www.habitat.org/
29	Real People Ltd	Credit-Only MFI	Nairobi County	https://realpeople.co.ke/
30	Neema Health Educational & Empowerment Programme (NEEMA – HEEP Ltd)	Credit-Only MFI	Embu County	https://www.neemaheep.org/
31	Ushindi Bora Ltd	Credit-Only MFI	Nairobi County	https://www.ushindibora.com/
32	Hand in Hand Eastern Africa	Credit-Only MFI	Nairobi County	https://handinhand-ea.org/
33	Nyali Capital Limited	Credit-Only MFI	Nairobi County	http://www.nyalicapital.co.ke/
34	Premier Credit Limited	Credit-Only MFI	Nairobi County	https://www.premierkenya.co.ke/
35	MoneyWorth Investment Limited	Credit-Only MFI	Nairobi County	
36	Hazina Development Trust Limited	Credit-Only MFI	Mombasa County	http://www.hazinagroup.co.ke/en/
37	SpringBoard Capital	Credit-Only MFI	Thika	http://www.springboardcapital.co.ke/
38	Progressive Credit Ltd	Credit-Only MFI	Nairobi County	https://progressivecr.com/
39	Longitude Finance	Credit-Only MFI	Nairobi County	http://www.longitudefinance.co.ke/
40	Jiweze Ltd	Credit-Only MFI	Nakuru	https://jiwezelimited.com/
41	ASA Ltd	Credit-Only MFI	Nairobi County	https://kenya.asa-international.com/
42	Kipepeo Microcredit Limited	Credit-Only MFI	Nairobi County	https://kipepeosolutions.co.ke/portfolio/
43	Liberty Afrika Technologies Limited	Credit-Only MFI	Nairobi County	https://www.libertyafrika.co.ke/
44	Diversity Microcredit Ltd	Credit-Only MFI	Nairobi County	http://www.diversitymicrocredit.co.ke/
45	My Credit Ltd	Credit-Only MFI	Nairobi County	https://www.mycredit.co.ke/
46	PAWDEP	Credit-Only MFI	Kiambu	https://www.pawdep.org/
47	Momentum Credit	Credit-Only MFI	Nairobi County	https://momentumcredit.co.ke/
48	Weighbridge Ventures ltd	Credit-Only MFI	Thika	
49	Micro Enterprises Support Program Trust (MESPT)	Wholesale MFI	Nairobi County	https://mespt.org/
50	OIKO Credit	Wholesale MFI	Nairobi County	https://www.oikocredit.coop/en/

Appendix IV: Ethics Review Approval

Strathmore UNIVERSITY

16th May 2022

Mr. Kiganda Moses,
moses.kiganda@strathmore.edu

Dear Mr. Kiganda,

RE: An Assessment of The Factors Affecting Cyber Resilience in Microfinance Institutions in Kenya

This is to inform you that SU-IERC has reviewed and **approved** your above **SU Masters'** research proposal. Your application reference number is **SU-IERC1324/22.** The approval period is **16th May 2022 to 15th May 2023.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-IERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-IERC within 48 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-IERC within 48 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to SU-IERC.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

for: **Dr Ben Ngoye,**
Secretary; SU-IERC

Cc: Prof Fred Were,
Chairperson; SU-IERC

STRATHMORE UNIVERSITY INSTITUTIONAL ETHICS REVIEW COMMITTEE
(SU-IERC)
16 May 2022
Email:ethicsreview@strathmore.edu
P.O BOX 59857-00200
NAIROBI-KENYA

Appendix V: NACOSTI Research Licence

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **467909**

Date of Issue: **09/April/2022**

RESEARCH LICENSE

This is to Certify that Mr.. Moses Kiganda Edemba of Strathmore University, has been licensed to conduct research in Nairobi on the topic: AN ASSESSMENT OF THE FACTORS AFFECTING CYBER RESILIENCE IN MICROFINANCE INSTITUTIONS IN KENYA for the period ending : 09/April/2023.

License No: **NACOSTI/P/22/16808**

467909

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013

The Grant of Research Licenses is Guided by the Science, Technology and Innovation (Research Licensing) Regulations, 2014

CONDITIONS

1. The License is valid for the proposed research, location and specified period
2. The License any rights thereunder are non-transferable
3. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research
4. Excavation, filming and collection of specimens are subject to further necessary clearence from relevant Government Agencies
5. The License does not give authority to tranfer research materials
6. NACOSTI may monitor and evaluate the licensed research project
7. The Licensee shall submit one hard copy and upload a soft copy of their final report (thesis) within one year of completion of the research
8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice

National Commission for Science, Technology and Innovation
off Waiyaki Way, Upper Kabete,
P. O. Box 30623, 00100 Nairobi, KENYA
Land line: 020 4007000, 020 2241349, 020 3310571, 020 8001077
Mobile: 0713 788 787 / 0735 404 245
E-mail: dg@nacosti.go.ke / registry@nacosti.go.ke
Website: www.nacosti.go.ke