UNIVERSITY OF NAIROBI

DEPARTMENT OF COMPUTING AND INFORMATICS

EFFECTIVE CYBER INCIDENT RESPONSE CAPABILITY FRAMEWORK FOR COUNTY GOVERNMENTS IN KENYA: A CASE OF MIGORI COUNTY.

BY

CAVIN ODHIAMBO OUMA

A RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN DISTRIBUTED COMPUTING TECHNOLOGY OF THE UNIVERSITY OF NAIROBI.

NOVEMBER 2021

DECLARATION

I declare that this research project report is my original work and has not been submitted elsewhere for examination, award of degree, or publication.

Signature  Date 24/11/2021

CAVIN ODHIAMBO OUMA

P53/12547/2018

This research project report has been submitted for examination with my approval as the university supervisor

 Signature: Date 24/11/2021

For Ms Pauline Wambui

Department of Computing and Informatics

University of Nairobi

DEDICATION

This thesis is dedicated to my parents who encouraged me on the value of education and without whose steadfast support, it would have not been possible to get this far.

ACKNOWLEDGMENT

First and foremost, I am grateful to Almighty God for the gift of placidity, good health, and countless blessings throughout my studies. Secondly, I wish to sincerely thank my supervisor Ms Wangunyu Pauline Wambui, who worked with me in the initialization and setting up the foundation of the project, and for her guidance without which the research would have not been a reality. Special thanks also go out to Professor Elisha Toyne O Opiyo for his expert reviews, contributions, and criticism that helped shape the direction of the research. I extend my sincere thanks to the academic and non-academic staff members of the University of Nairobi, for their support and for ensuring a smooth learning environment. Lastly, to my family, I am because of you. You have continuously prayed and supported me throughout my studies.

Thank you and God bless you all.

ABSTRACT

The increased adoption of ICT in the Kenyan County Governments has led to increased cyber incidents within the counties. Response coordination and management of cyber incidents nationally and locally is the responsibility of the National Kenya Computer Incident Response Team - Coordination Centre (KE-CIRT/CC). However, county governments are often unaware of the risk because of the assumption that the management of information systems security and addressing the risks are the responsibilities of the national government. In addition, there are new cyber incidents faced locally due to the devolved ICT-enabled infrastructures that require a localized approach. This research was informed by the two factors; increased cyber incidents and threats at the county level due to the devolved ICT-enabled services and the lack of localized cyber incident response framework to respond to cyber incidents at the county level. To address the two mentioned concerns, this study sought to develop a localized cyber incident response capability framework from a study that targeted a total population of 121 Migori County Staff. Consequently, the study adopted descriptive approaches augmented by quantitative techniques to measure the variables. A sample size of 93 was obtained using Yamane's formula out of whom 76 responded. The study analyzed the collected data using Microsoft Excel, Google Forms, and SPSS to derive descriptive statistics and to perform ordinal regression. The study found that all the four independent constructs; policies, risk management, resources, and training, had a positive correlation coefficient with the dependent variable effective cyber incident response capability. The developed framework can be used to guide and manage cyber incident response in the county governments in Kenya.

Key terms: Cybersecurity, Cybersecurity Framework, cybercrime, incident response,

Table of Contents

LIST OF TABLES

TABLE OF FIGURES

LIST OF ABBREVIATIONS

AU-African Union

BCP-Business Continuity Plan

CA- Communications Authority

DRP-Disaster Recovery Plan

ICT- Information Communications Technology

IFMIS- Integrated Financial Management Information System

IoT-Internet of Things

KE-CIRT/CC -The National Kenya Computer Incident Response Team - Coordination Centre

NPKI- The National Public Key Infrastructure (NPKI)

NSSF- Nationa Social Security Fund

ISO- The International Organization for Standardization

SPSS- Statistical Packages for Social Sciences

CHAPTER ONE: INTRODUCTION

1.1 Overview

In the past decade, both public and private sectors have witnessed a rapid climb in the use of Information Communications Technology (ICT). Internet penetration in Africa grew from 5% in 2007 to 28% in 2015 with Africa expected to reach comparable internet access rates to the developed world (AU, 2016). The increased proliferation of smartphones, applications and the penetration of the internet has virtually impacted every sector including the local governments. According to Thompson (2019), technological developments have transformed local governments across different locations by providing increased transparency and streamlined operations. In Kenya, internet penetration has greatly improved with and the overall cost of the internet has become cheaper, internet speeds have also become faster (Kiboi, 2015). ICT use has become a matter of strategic importance and is a key driver of government development goals according to 'Kenya Vision 2030' National Development Plan (Ministry of ICT, 2014).

The introduction of devolution and the County Governments following the 2010 Constitution has increased the incorporation of ICT into various critical factors at the county level (Serianu, 2014). However, the increased adoption of technology has exposed the Kenyan National and County Governments, the private sector, and society to cybersecurity threats (Kiboi, 2015). Cybersecurity is considered an emerging threat to national security. Kenya placed the national cyber-security framework in response to increasing Cybersecurity vulnerabilities as a strategy to protect the country's ICT assets as well as overall management of cybersecurity in the country (Matinde, 2014). However, since then, Cybersecurity incidents have continued to occur across the country.

Cybersecurity is increasingly becoming important at the county levels with the growing adoption of new technologies and online integrated services. This necessitates the need to have adequate incident response capabilities in the event of such cyber-attacks at the county levels.

This paper seeks to develop a localized framework for effective cyber incident response capability at the county level. Specifically, the research will focus on Migori County. This research will address the gap that is viewed as a lack of localized cyber incident response framework specific to the County Governments. The concepts herein will build upon various insights that have been undertaken by various researchers in the topic area of cybersecurity threats and frameworks in national and local governments.

1.2 Statement of Problem

Most cyber incident response reports and frameworks are produced by international cyber-security firms which lack local depth and breadth (Mayunga, 2020). County governments in Kenya face massive Cybersecurity risks owing to weak or nonexistent Cybersecurity frameworks (Waithaka, 2016). According to Chitehi et al (2018), cyber-attacks increased by 108% nationally and county governments lacked better initiatives on cyber response. The county governments are often unaware of the risk because of the assumption that the management of information systems security and addressing the risks are the responsibilities of the national government through The National Kenya Computer Incident Response Team - Coordination Centre (KE-CIRT/CC) (CA, 2020). In addition, ICT is dynamic and has different levels of adoption. These and the inadequate cyber response capabilities by the counties call for a localized standard framework for ensuring effective cyber incident response capabilities at the county level.

1.3 Background of Study

According to the Information Systems Audit and Control Association (ISACA) State of Cybersecurity 2020, cyber-attacks continue to increase globally and are often underreported (ISACA, 2020). Similarly, Allen (2021), found that Africa is facing evolving cyber threats. Countries also face different cyber threats depending on their internet penetration and adoption of technology. Owing to her increased dependence on ICT, Kenya is exposed to cyber-attacks that threaten its national security (Kiboi and Kiboi, 2015). With the devolution and introduction of county governments in Kenya, cybercriminals have discovered new targets for attacks. While many of the studies have focused on cybersecurity threats to national, continental, and global security, the development of a strong culture of Cybersecurity and creating robust response capabilities begin from the grassroots levels. This study will focus on the cyber threats and incident response capabilities at the county level specifically Migori County and develop a localized Cybersecurity framework for managing and mitigating Cybersecurity threats and attacks within the county.

1.4 Objectives

1.4.1 Main Objective

To develop an effective cyber incident response capability framework for county governments in Kenya.

1.4.2 Specific Objectives

1. To investigate the influence of policy on effective cyber incident response capability at the county level.
2. To investigate the influence of risk management on effective cyber incident response capability at the county level.
3. To investigate the influence of resources on effective cyber incident response capability at the county level.
4. To investigate the influence of cybersecurity training on effective incident response capability at the county level.
5. To formulate a framework for effective cyber incident response capability at the county level.

1.5 Research Questions

1. What are the major cyber incidents faced by the county governments in Kenya?
2. What variables are necessary for evaluating the cyber incident response capabilities of county governments in Kenya?
3. What are the indicators for measuring effective cyber incident response capabilities by the county governments?

1.6 Significance of the Study

According to a report by the Communications Authority of Kenya (CA) on National Threat Landscape during the period October-December 2019, there were 37.1 million cyber threat events detected by (CA, 2020). The Kenyan Government's economic blueprint, "Vision 2030' aims at achieving universal access to ICTs as one of its major objectives (Ministry of ICT, 2014). Consequently, the Kenyan Government introduced several online-enabled services such as e-citizen services and Integrated Financial Management Information System (IFMIS) which have been further devolved to the County Governments. The increased dependence on ICT means exposure of the private sectors and the general society within these counties to cybersecurity risks which can affect the county governments. To mitigate the impacts of cyber incidents at the county level, there should be an incident response plan to enable the continuation of critical services and reduce time and levels of interruption.

1.7 Limitations of Study

There is a limited number of scholarly articles and primary sources on Cybersecurity frameworks and incident response capabilities in county governments in Kenya. Most counties also often do not report any cyber incidents that occur at the county levels or their response to such incidents. This research proposes dynamics of a framework for ensuring effective incident response capabilities at the county level. However, since the dynamics rely on technological factors and the level of adoption of technology which is increasingly changing, the cyber incident response framework measurements proposed herein may need frequent review and update. Lastly, due to the difficulty of reaching targeted respondents during the Covid-19 pandemic, there is a likelihood of response bias.

1.8 Theoretical Framework

1.8.1 International Relations Theory

Cybersecurity is a growing field and the cyberattack surface is very wide. Modelling and constructing cyber incident response frameworks borrows from different theories mostly from International Relations theoretical frameworks (Kleinberg et al., 2015). The theory is divided into three levels of study; the international system, state, and the sub-state level all derived from Political Science and National Security fields. In the development of a better cybersecurity model, all levels of IR theory must be considered together. This is because of the anonymity provided by the internet allowing the attacker to be able to mask their identity or make it hard to find, the internet also allows for one individual with good IT knowledge to potentially challenge cybersecurity at all levels, and lastly, the internet offers instant global access allowing any individual or organization to a perform a cyber-attack from anywhere and on any target. Lastly, cyberspace is inherent hence no one individual or organization can completely control the whole or substantial part of it while operating at a particular level of IR theory. This theory informs the proposed construct of policies which shall include international cybersecurity standards and national and county level laws and legislations.

1.8.2 Classical Realism Theory

This research uses the Classical Realism theory which is based on the paradigm that “Human nature is unchanging and evil.” As a result, conflicts of interest are inevitable; thus, conflicts are inevitable” (Walt, 1998). The research follows the Offense-Defense sub-theory of Classical Realism which according to Walt (1998) is the critical balance between offence and defence. There is little security and cyber resilience in an ICT environment where the offence has the advantage.

On the contrary, cybersecurity is better in an environment where the defence has the advantage. Cybersecurity is offence-dominant since the increased adoption of technology makes defence alone not a guarantee from cyber attacks. The goal of developing a cyber incident response framework is to reduce the impact of the increasing number, type, and severity of attacks.

1.8.3 Game Theory

This research also borrows from Game Theory which is based on the paradigm that for every adversarial action, a countering defence strategy needs to be defined. The cyber incident response framework must thus be as adaptive as the cyberthreats can be. The goal of developing a cyber incident response framework based on proactive defence is to ensure that systems can recover faster and effectively from shocks caused by cyber-attacks. Game theory informs the proposed construct of risk management which involves using the predictive power of game theory to perform risks and vulnerability assessments and management.

1.9 Conceptual Framework

Various models and frameworks for cyber security and incident response were modified to suit the inquiry. In the development of its conceptual framework, this research used constructs borrowed from the definition of cybersecurity by ITU, Serianu cybersecurity framework, ISACA guidelines on IT Governance and Management, and The National KE-CIRT/CC Framework in defining the Cyber incident capabilities of the County Government of Migori.

Table 1.1: Old Frameworks and Proposed Framework Constructs

Serianu	**The National KE-CIRT/CC Framework**	**Change**	**Proposed Constructs**
Governance and Strategy	National Policies, Laws, and Regulations	Amended	1). Policies
Vulnerability and Threat management	Early warning and technical advisories	Amended	2). Risk Management Approaches
User Provision and Access Management	Technical Coordination and Response to Cyber Incidents	Amended	2). Risk Management Approaches
Continuous Monitoring and Incidence Response	Awareness and Capacity Building	Amended	3). Training
	Development and Implementation of NPKI	Amended	2). Risk Management Approaches
	Establish collaborations on cybersecurity	Amended	4). Resources
	R&D on Cybersecurity	Amended	4). Resources

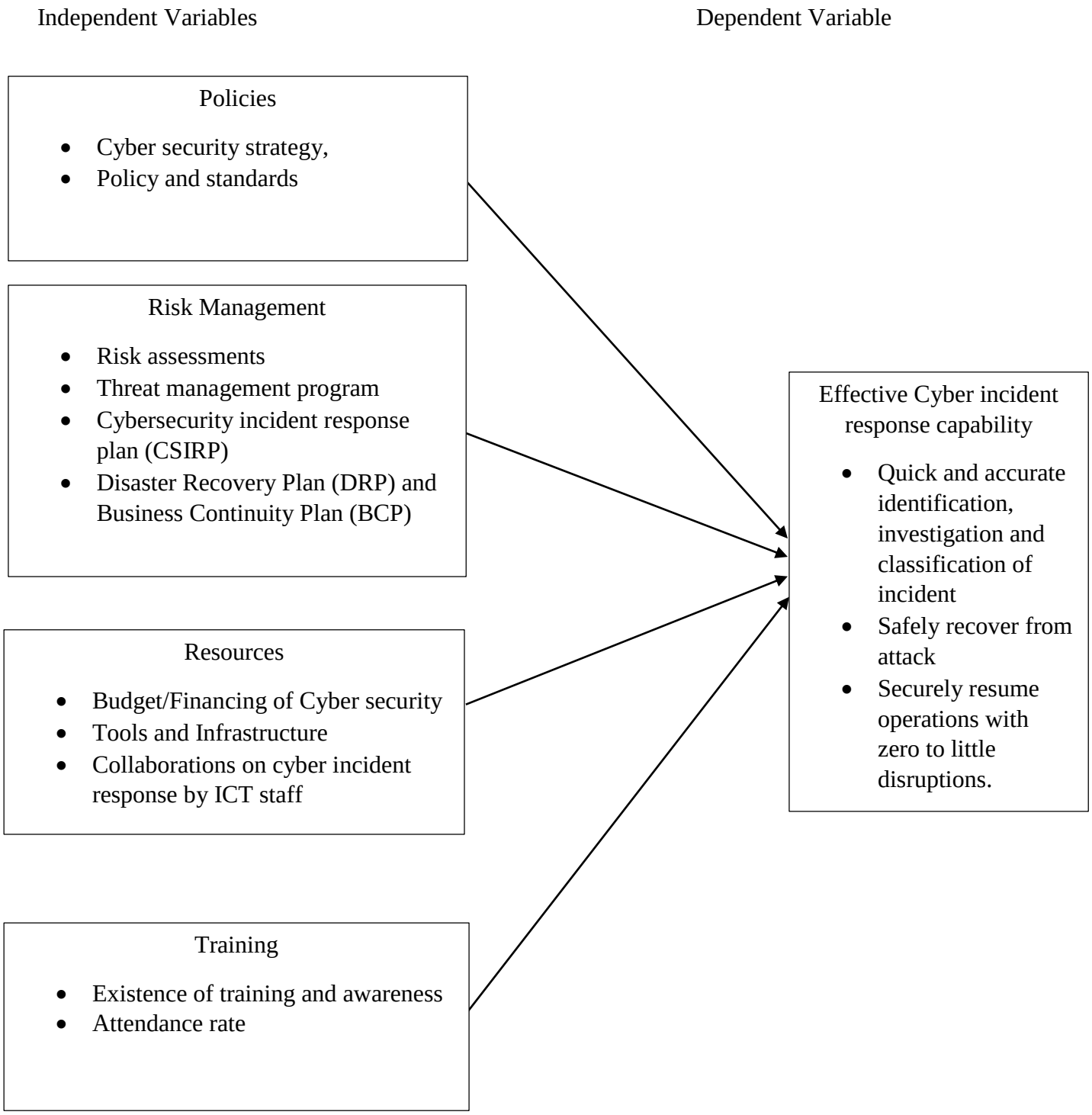

Figure 1. 1: Conceptual Framework Diagram

1.10 Operationalization of Variables

Table 1. 2: Table of operationalization of variables

Variables	Indicators	Measurement
Policies	Cyber security policy, strategy, and standards. Cybersecurity certifications/standardization legislation or regulations	Evidence of Policies Compliance. Evidence of Compliance to cyber security strategy and standards. Evidence of compliance to legislations or regulations.
Training	Presence of training. Attendance of training	How frequently does the county conduct cybersecurity training? The number of employees who attend cybersecurity awareness training.
Resources	Budget/Financing of Cyber security. Tools and Infrastructure. Collaborations on cyber incident response by ICT staff	Percentage of county budget allocated to Cyber incident response measures. Evidence of collaborations on cyber incident response by ICT staff.
Risk Management	Cyber Risk assessments Threat management program Cybersecurity incident response plan (CSIRP) Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP)	Cybersecurity Audit Reports Evidence of Threat management programs. Evidence of CSIRP. Recovery Point Objective Recovery Time Objective
Effective Cyber Incident Response Capabilities	Quick and accurate identification, investigation, and classification of an incident. Safely recover from an attack. Securely resume operations with zero to little disruptions.	Acceptable downtime. 99.9 percent uptime. Acceptable data loss

The study identified four variable constructs as independent namely; policies, risk management, resources, and training. These independent variables were conceptualized to have an effect on the dependent variable which was effective cyber incident response capability. Effective cyber incident response capability was modelled as the dependent variable dependent upon the four independent variables. Therefore, improvements or deterioration of the four independent variables should impair or enhance cyber incident response capability. The research collated a set of metric variables relevant to the cybersecurity operating environment for the county government of Migori for each of the identified constructs. The metric variables informed the survey instrument which was designed to evaluate the cyber incident response capabilities of the county government of Migori. The level of impact each construct has on cyber incident response capability was measured via statistical methods.

1.11 The hypothesis of the Study

According to Kothari (2004), a hypothesis is a proposition defined to explain the occurrence of a specified phenomenon, either inserted as a provisional conjecture either to guide research or be accepted as plausible in light of derived facts. The hypothesis measures relationships between the variables being studied. The research chose the following null hypothesis for carrying out the study based on the conceptual framework.

$H0_1$ Policy factors do not have an effect on effective cyber incident response capabilities at the county level.

$H0_2$ Risk management factors do not have an effect on effective cyber incident response capabilities at the county level.

$H0_3$ Resources factors do not have an effect on effective cyber incident response capabilities at the county level.

$H0_4$ Training factors do not have an effect on effective cyber incident response capabilities at the county level.

2 CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The proliferation of the internet, adoption of smartphones, improved mobile networks, and other related information and communications technologies (ICTs,) have provided new prospects for governments, private businesses, civil societies, and individuals globally to operate and increase their communication and presence. In Africa, the gains in technology have been associated with tremendous economic developments (AU, 2016). Increased adoption of ICT has also introduced new ways for criminals to circumnavigate the ICT systems and expose the governments, organizations, and people to cybersecurity risks. With increased interconnectedness and dependency on ICT comes more vulnerability hence the need to ensure the continuous security of the ICT infrastructure to maintain its integrity as well as end users' trust in its reliability. According to Allen (2021), cyber threats in Africa could be underestimated since a majority of cyber incidents are either unreported or unresolved.

A cyber incident is an unexpected event that can disrupt normal operations and affect the productivity of users (Shinde and Kulkarni, 2021). Consequently, cybersecurity can be defined as guarding the information systems, organization, and related assets through strategies, plans, measures, training, and practices (ITU, 2014). The devolution of more IT-enabled services to local governments increases their vulnerability to a cyberattack (Thompson, 2021). The Kenyan government formulated County Governments following the enactment of the new constitution in 2010 (ROK, 2010). These county governments have become the centres for access to functions previously under the national government. Devolving some ICT-enabled services from national to county governments meant increased investments in ICT at the county level to offer similar or near-similar levels of services as previously offered by the national government. The demand for uninterrupted access of the devolved ICT services has increased necessitating measures to ensure

minimum interruptions in case of a cyber incident. The reactive process of restoring processes to normal operations in an event of a cyber incident is a cyber response.

As a result, this research benefits from both worlds of a localized framework incorporating international standards. The first step to improving cybersecurity within the county governments is recognizing vulnerabilities. According to Thompson (2019), as compared to national governments, the local governments lack a complete cybersecurity landscape in their ICT systems. An analysis of the existing models and frameworks and the increase in cyberattacks in Kenya and more so localized attacks show either the lack of implementation of the frameworks or their lack of applicability at the county level hence not being able to protect cyber infrastructure adequately.

2.2 Empirical Review Literature

Cyber incident response is the methodological application of cyber attack management strategies to minimize potential impacts on business processes, customers, and intellectual property (Hove et al. (2014). Antonucci (2017) documented the idea of modelling cybersecurity frameworks and found that there was a lack of unanimity on which standard or framework suits all specific situations (Antonucci, 2017). While several studies have been done in regards to cybersecurity in Kenya focusing on national and government ministries (Waithaka, 2016), only a few studies have focused on cybersecurity at the county level. According to Koech (2016), the county governments found key Information Systems frameworks in existence to be unimplementable due to their complexity and costs hence they needed a simple framework that would still be effective and can be employed at minimum effort.

A Study by Chitehi et al (2018) found that due to the cybersecurity challenges faced by the County Governments in Kenya, there was a need for them to enact policies, perform cybersecurity

awareness training, and have management support through adequate allocation of resources to cybersecurity measures. However, the implementation of such measures required the development of a Cybersecurity framework based on comprehensive risk assessment within the county governments.

Consequently, Chitehi et al (2020) developed a model for assessing cybersecurity vulnerability for county governments in Kenya while focusing on Kakamega and Bungoma Counties. The study borrowed the definition of vulnerabilities from Abomhara and Koien (2014) which defined them as weaknesses in an organization's systems such as the county government that can allow intruders to access and perform system attacks. The study found that support and funding, policies and regulations, and technology were the main factors that affected cybersecurity. While the developed model targeted reducing cyberattacks at the county level, it did not explain actions to take in case of successful cyber attacks.

2.3 Existing Approaches to Cyber Attack Management

Accordingly, Serianu (2017) suggested that Kenya should develop her core Cybersecurity and cyber-resilience philosophies, unique to the Kenyan ecosystem, instead of borrowing heavily from international best practices. To ensure effective cyber attack management, several frameworks and measurement matrics for quantifying Cybersecurity readiness have been published in some standards and literature. In Kenya, several cybersecurity frameworks local and international have been adopted for Cybersecurity which includes:

2.3.1 National Computer Incident Response Team Coordination Center (KE-CIRT/CC) Cybersecurity Framework

The Communications Authority of Kenya (CA) has pushed through legislation for Cyber-crime including the Kenya Information and Communication KICA Act, 1998, Kenya Information and Communications (Cybersecurity) Regulations, 2016, and Computer Misuse and Cybercrimes Act 5 of 2018 (suspended by a court in 2019). The CA was mandated by the KICA Act (1998) to develop a national cybersecurity management framework. They established the national Computer Incident Response Team (CIRT). The National Kenya Computer Incident Response Team Coordination Center (National KE-CIRT/CC) was established by the Communications Authority and was tasked with response coordination and management of cybersecurity incidents nationally while also collaborating with relevant actors locally.

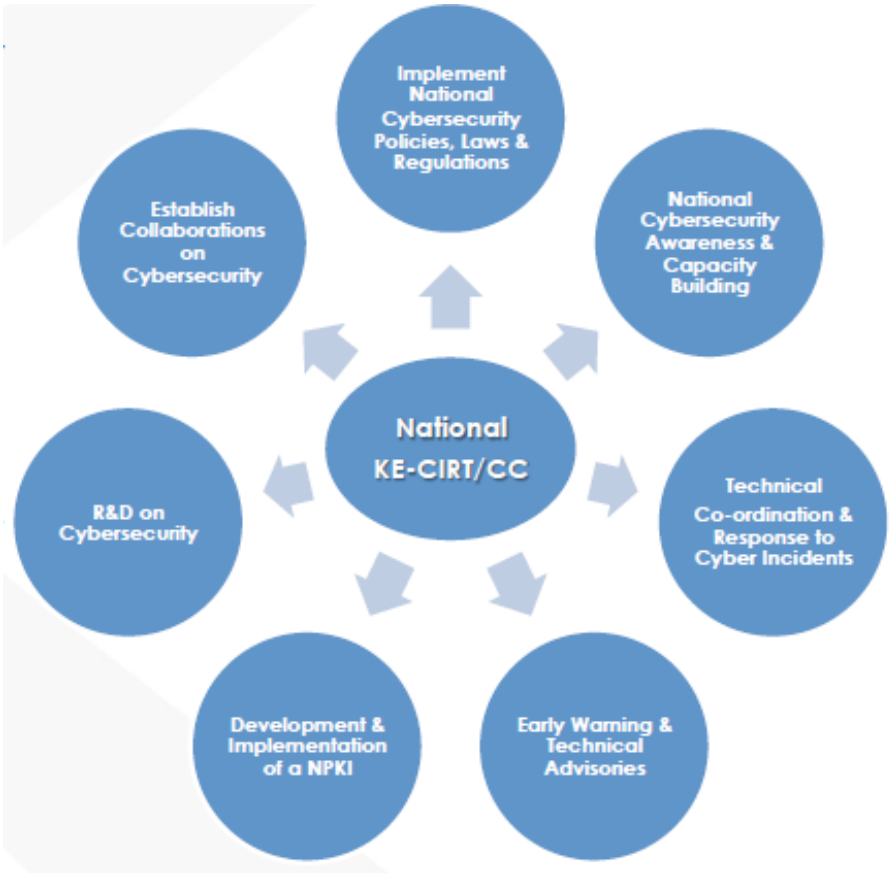

Figure 2 1: The National KE-CIRT/CC Framework (CA, 2020).

2.3.2 NIST- Framework for Improving Critical Infrastructure Cybersecurity v1.1

This framework was developed by the National Institute of Standards and Technology (NIST) as an update to the v1.0 developed in 2004 by the same organization (NIST, 2018). This is one of the most common frameworks globally and offers a flexible way of addressing cybersecurity and its impacts (NIST, 2018). NIST framework has four broad categories of Identify, Protect, Detect, Respond and Recover. These categories are further subdivided into twenty-one sub-categories.

2.3.3 Serianu Cyber Security Framework

The framework was developed by Serianu Ltd., a Kenyan-based IT services company specializing in information (cyber) security services in Africa (Serianu, 2015). Serianu cybersecurity research studies are based on their baseline controls, collectively known as the Serianu Cyber Security Framework (Serianu, 2015). Though built for regional suitability, the framework has incorporated best practices from COBIT, ISO 27001, SANS 20 Controls, and NIST. The Serianu Cyber Security Framework consolidates controls into four categories, namely: Vulnerability and threat management, cybersecurity program governance and strategy, continuous monitoring and incident response, and user provision and access management (Serianu, 2015).

2.4 Overview of Migori County Government ICT

Migori County covers 2500 square kilometres and borders Tanzania to the South and Uganda to the West, The county comprises 10 Sub-Counties namely, Rongo, Awendo, Suna east, Suna West, Uriri, Nyatike, Kuria East, Kuria West, Ntimaru, and Mabera (Migori County Government, 2021). The County Government of Migori has invested in providing tools to enable efficient and accountable ICT-enabled services. The vision of Migori County ICT Roadmap is to be a " vibrant, modern and regional commercial hub with a high standard of living for her residents through the use of ICTies'," (ICTA, 2015). Migori County's ICT department is under the Directorate of ICT and E-Governance, Office of the Governor (Migori County Government, 2021). The key departments in the county that use ICT-enabled services include the Public Service Boards, Salaries and Revenue, Procurement, Administration, and the ICT departments.

3 CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodologies which were used in this research to meet the objectives defined in chapter one. The research sought to develop a cyber incident response capability framework for the County Government of Migori. The chapter is divided into the following sections; research design, target population, sample and sample size, data collection, analysis, reliability and validation, and ethical considerations.

3.2 Research Design

Research design serves to formulate procedures and processes necessary for a quality study judged by its validity, objectivity, accuracy, and ethics (Kumar, 2011). The study adopted a descriptive research design augmented by quantitative techniques to measure the variables. Quantitative approaches were appropriate to meet the study's objectives precisely defined in chapter one. The study chose a descriptive design because it sought to establish only associations between the identified variables.

The 2010 Kenya Constitution created 47 County Governments and devolution of services which has increased the incorporation of ICT into various critical factors at the county level (Serianu, 2015). Migori county was chosen as the focus for the study due to similar structure and key functions within the county governments.

3.3 Target Population

Kumar R (2011), defines the target population as the people (individuals, groups, and communities) that meet the sampling criteria to be included in the study. Due to the centralized nature of the devolved IT-enabled services at the county headquarters (Tödtling et al., 2018), the research considered those employees who perform their daily activities within the headquarters and interact with IT systems in their day to day activities. This reached a target population of 121 employees who work in the departments of ICT, Salaries and Revenue, Administration, Public Service Board, and Procurement which fall in the sub-sectors: Governor's office, County Assembly, Public Service, and Finance and Economic Planning (Migori County, 2018).

3.4 Sample and Sample Size

The research sample defines the members of the target population from whom data is collected. The study used purposive sampling. The research carefully selected people who were competent and could contribute new ideas to the research problem. The sampling point was the County headquarters offices of Migori County. The sampling design was chosen based on the subject matter, nature of data to be collected, objective of the research, and target population's size.

According to Kothari (2009), good sample size is goal-oriented, efficient, flexible, reliable, and represents the entire study population. Yamane's formula shown below (Yamane, 1973) was used in determining the sample size for this study.

$$n = \frac{N}{1 + N(e^2)}$$

n is the desired sample size of the study population,

N is the total study population,

e is the level of statistical significance level

The confidence level is expressed in percentage or decimal and provides a probability that the results will be reliable and hold to the population sampled. The formula used a confidence level of 95%.

$$n = \frac{N}{1 + N(e^2)}$$

$$n = \frac{121}{1 + 121(0.05^2)} = 93$$

3.5 Data Collection

This research used a self-administered questionnaire as the data collection instrument. The respondents were interviewed through a self-administered questionnaire consisting of a series of close-ended questions. The choice of the questionnaire was guided by the fact that the instrument can be mailed through the internet, collectively administered, or administered in public or online platforms (Kumar, 2011). In addition, the number of questions involved in the research and the reduced cost of implementing them through an online self-administered questionnaire informed the choice (Durga et al., 2019). This makes the instrument more convenient and less costly to administer since the intended respondents can easily be reached. The questionnaires were designed using Google forms and distributed to the respondents electronically using emails containing the URL link. Personally identifying information and email addresses of respondents were not collected upon their submission of questionnaires.

The metric variables identified in the conceptual framework were presented to the respondents as questions. Closed-ended questionnaires were used in the form of single-choice radio buttons, multiple-choice checked-boxed types, and multiple Likert scales matrix questions. Each response had a numeric value based on a scale. Likert scale is a psychometric response scale of five points

that allow respondents to select point reflective of their level of agreement to a statement (Joshi et al., 2015).

Table 3 1: Likert 5-Point Scale

Grading		Weighted Mean score	Grading ranking strength
Strongly Disagree	No extent	<=1	1
Disagree	Little extent	> 1 and <= 2	2
Neutral (Neither Agree nor Disagree)	Moderate extent	>2 and <=3	3
Agree	Large extent	>3 and <=4	4
Strongly Agree	Very large extent	>4 and <=5	5

3.6 Reliability and Validity

In checking for the reliability and validity of questionnaires administered to the study sample, the instrument was pre-discussed with the supervisor to review its design, content, layout, appropriateness, and objectivity. The research used objective questions that measured the concepts defined in the conceptual framework and represented what respondents know about cyber incident response. The paper used *Spearman's* rank-order Correlation Coefficient using a valid measure of 0.05 to ensure validity.

3.7 Ethical Consideration

The county staffs are very sensitive about releasing county government information. As such, appropriate measures were taken to instil confidence in the participants. First, respondents were informed of their rights to the study. It was made clear to the respondents the voluntary nature of

their participation and the right to withdraw from the study at any moment. In addition, their names and any other personally identifying information were neither collected nor used in any publication or presentation. An oral and or written consent was obtained before interviews.

3.8 Data Analysis

A number of analysis tools and statistical analysis methods were used based on their suitability to achieve research objectives and appropriateness in answering the research questions. Google form provided data collection and analysis capabilities. The data was converted into a Microsoft Excel spreadsheet to analyze and draw graphs. For the descriptive statistical analysis, IBM Statistical Package for the Social Sciences (SPSS) was used. Spearman correlation was used to present the state of cyber incident response capability and considered the development of the county's cyber incident response capability framework.

4 CHAPTER FOUR: ANALYSIS AND DISCUSSION

4.1 Introduction

The main objective of the research was to develop a framework for ensuring effective cyber incident response capability at the county level. The study used self-administered online questionnaires administered via Google forms to collect data. This chapter presents the results of the data collection, descriptive analysis, and discussion of the implications of the results.

4.2 Analysis

4.2.1 Response Rate

The target population for this study was 93 IT systems end-users across various departments within the county government of Migori. A total of 93 questionnaires were distributed via emails and social media platforms to the respondents. The questionnaire had 53 questions. Out of the 93 possible questionnaires, only 76 were filled and submitted. This represented an 82% response rate. A questionnaire return rate of 50% is adequate for data analysis and reporting; a rate of 60 percent is good and a response rate of 70% and over is excellent (Mugenda and Mugenda, 2003).

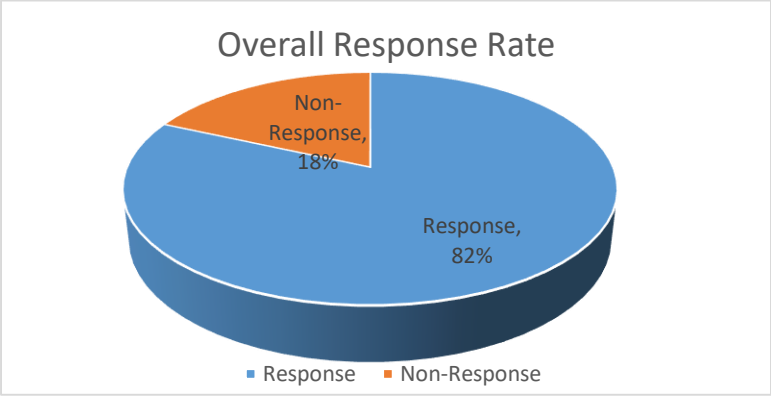

Figure 4 1: Overall Response Rate

4.2.2 Demographic Distribution of Respondents

The research sought to establish the general information of the respondents by asking them about their age, gender, education level, and credentials.

Table 4 1: Demographic Distribution of End Users

	Category	Frequency	Percentage	Valid percentage	Cumulative percentage
Gender	Male	45	59.21	59.21	59.21
	Female	31	40.79	40.79	100
	Total	76	100	100	
Age	18-24	9	11.84	11.84	11.84
	25-34	34	44.74	44.74	56.58
	35-44	24	31.58	31.58	87.51
	45-54	9	11.84	11.84	100
	Total	76	100	100	
Education	Certificate	1	1.32	1.32	1.32
	Diploma	17	22.37	22.37	23.69
	Degree	53	69.74	69.74	93.43
	Masters	5	6.58	6.58	100.00
	PhD	0	0	0	
	Total	76	100	100	
Departments	Public Service and Administration	14	18.42	18.42	18.42
	Information Communications Technology-ICT	25	32.89	32.89	51.31
	Roads, Transport, Public Works, and Energy	4	5.26	5.26	56.57
	Health Services	2	2.63	2.63	59.2

	Education, Youth, Sports, Cultural, and Social Services	12	15.79	15.79	74.99
	Finance and Economic Planning	10	13.16	13.16	88.15
	Trade, Tourism, and Co-operatives	2	2.63	2.63	90.78
	Agriculture, Livestock, Fisheries, and Water Development	2	2.63	2.63	93.41
	Lands, Housing, and Physical Planning	3	3.95	3.95	97.36
	Environment, Natural Resources, and Disaster Management	2	2.63	2.63	99.99
	Total	76	100	99.99	

From *Table 4.1* above of demographic distributions, male respondents constituted 59.21% while female respondents constituted 40.79% of the respondents. The results in regards to gender ratio can be attributed to male dominance in Migori County departmental employments (Awuor et al., 2018). The majority of the probed respondents were aged 25-34 representing 44.74% followed by those aged between 35-34 at 31.58%. There were no respondents aged above 54. The National Social Security Fund (NSSF) puts the official retirement age for public service employees at 60 (Muthaura, 2017). In regards to their level of education, a majority of respondents had a university degree as their highest level of education forming 69.74%. The lowest education level among respondents was a Kenya Certificate of Secondary Education (KCSE) certificate which was one respondent while the highest education level was a master's degree with 5 respondents representing 6.58%. Based on the departments that the respondents worked in, the majority were found to belong to the Information and Communication Technology (ICT) department at 32.89% followed closely by the Department of Public Service and Administration at 18.42%.

4.2.3 Cyber Incidents Landscape at the County Level.

When asked to rank the level of key cyber threats and attacks to the county government, natural and manmade disasters ranked highest in likely cyber threats to the county ICT infrastructure with an average of 3.83 followed by IT Systems failure at an average score of 3.43 as shown in *Figure 4.2* below. Human error was third at 3.2. The lowest level of threat was Ransomware according to a majority of the respondents at 1.22.

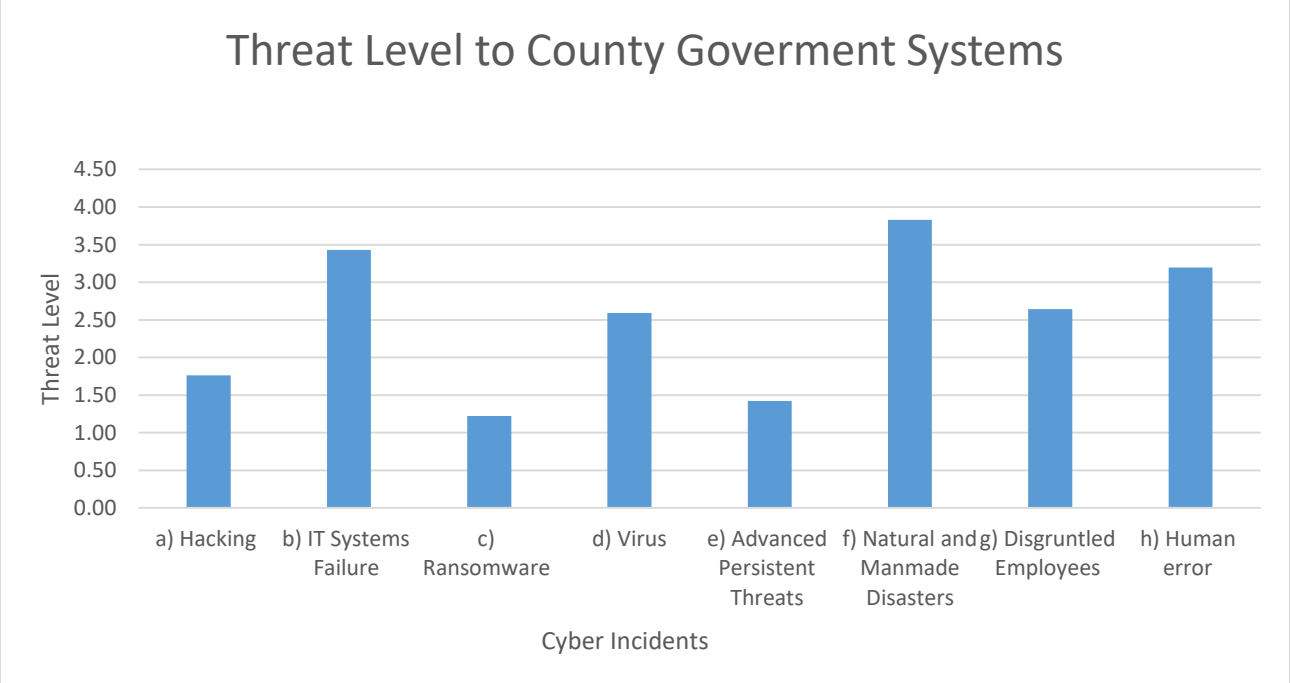

Figure 4 2 A graph of the threat level of various cyber incidents at the county level.

When asked about the volume and severity of the above-mentioned incidents at the county level, 55% of the respondents believed the volume of the identified cyber incidents had increased over the past two years while 34% also believed the severity of such incidents had increased over the same period.

4.2.4 Cyber Incident Response Capabilities of the County Government.

On ranking various factors on the county's cyber incident response capabilities, the respondents were asked to rank on a scale from 1(low) to 5(high) the county's ability to prevent, detect, contain, respond to attack, and ability to hire and retain cybersecurity personnel. The County Government's ability to respond to cyber incidents ranked lowest with a score of 1.55 followed by the ability to contain a cyber incident at 1.93 as shown in *Figure 4.3* below. The county had a near-average ability to contain cyber incidents at 2.43 and the ability to prevent at 2.05. The county's ability to hire and retain skilled Cybersecurity personnel was average at 2.83. Overall cyber incident response capability of the county was 2.03 which is low.

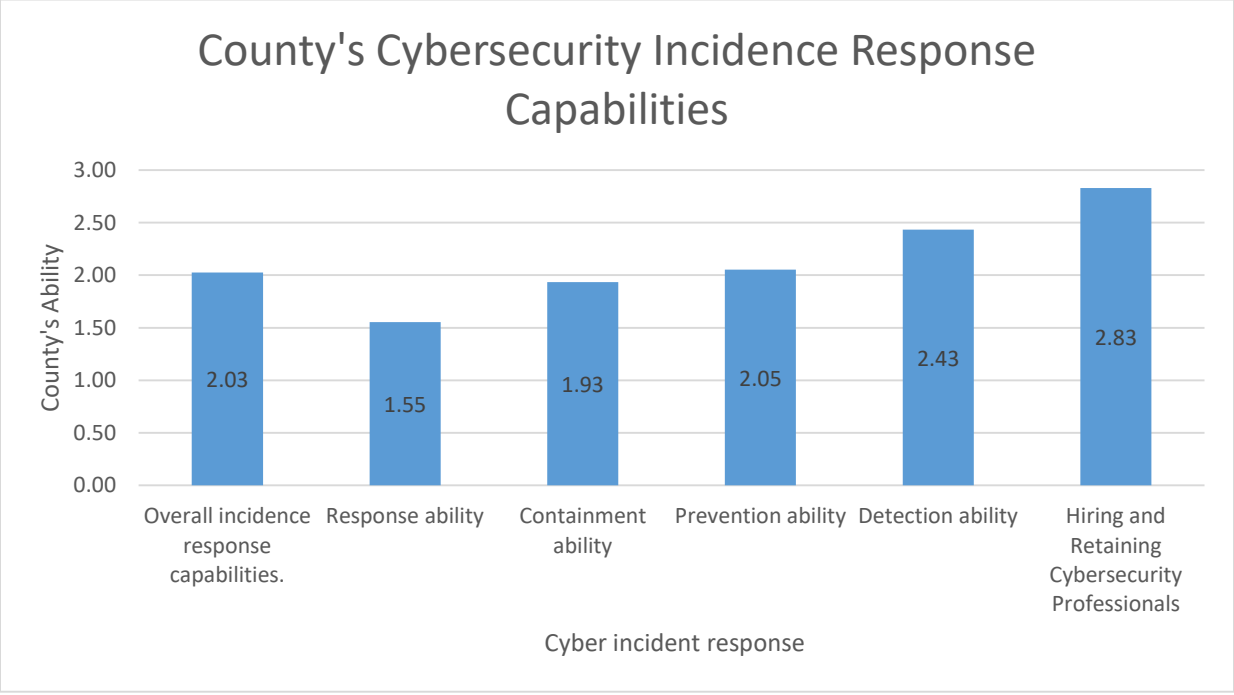

Figure 4 3: A graph of the county's cyber incident response abilities.

4.2.5 Analysis by Constructs

4.2.5.1 Policies

To measure this construct, several questions were fielded to the respondents and were used to rank the County Government's policies concerning ICT incident response capabilities. The respondents were asked whether they are aware of the existence of the County Cybersecurity policy. 22% of the respondents affirmed while 9% said no. 69% of the respondents were not sure if the county had a cybersecurity policy. Consequently, a follow-up question asked those who were aware of the existence of cybersecurity policy if they understood the policy. A majority of respondents at 48.9% mentioned that they did not understand the county's cybersecurity policy with only 8% saying they understood it.

The respondents were also asked if the county had Cybersecurity strategies aimed at addressing business risks. 76% of the respondents said the county had cybersecurity strategies aimed at addressing business risks, while 5 respondents representing 19.2% said they were not sure. Among the respondents who believed the county had cybersecurity strategies aimed at addressing business risks, 47.8% did not believe the strategies were effective in addressing the business risks while 43.5% were not sure. The County Government ICT has adopted Computer Misuse and Cybercrimes Act No. 5 of 2018 which all respondents were aware of with a 100% score. The level of compliance with the legislation averaged 3.43 out of 5. Respondents were also asked in a multichoice question, what factors they considered as barriers to adopting and implementing national or international Cybersecurity frameworks at the county level. Insufficient funding and lack of training of end-users were shared as the two major barriers at 80.8%. Inability to hire and retain skilled Cybersecurity personnel was the least barrier according to the respondents with only 11.5% choosing it. This is shown in *Fig 4.4* below.

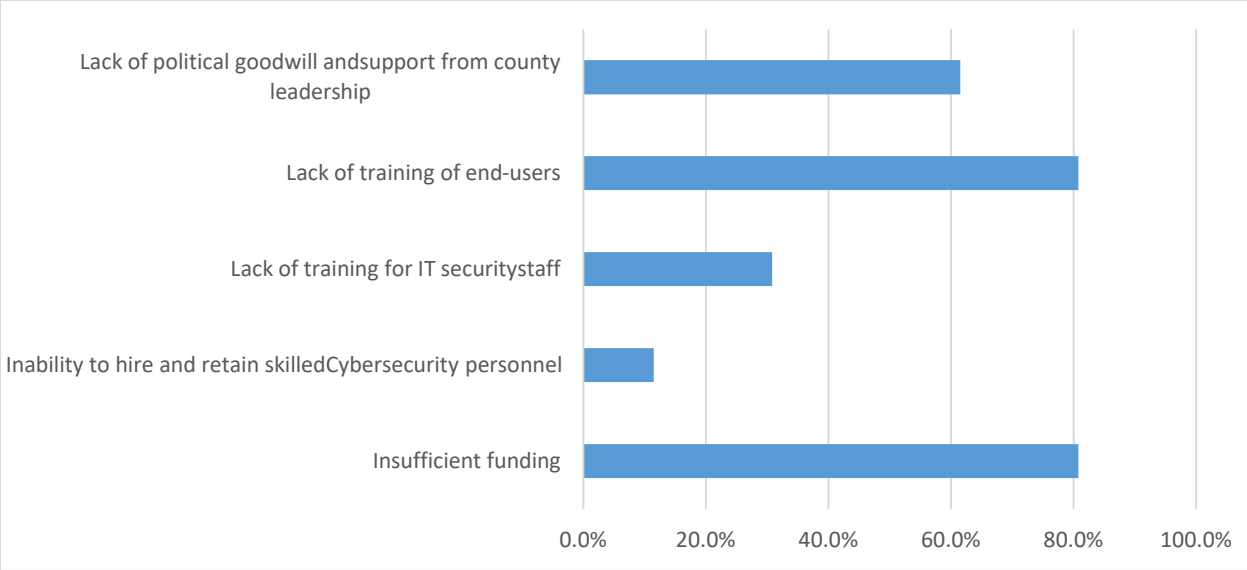

Figure 4. 4: Barriers to Cybersecurity frameworks implementation

4.2.5.2 Risk Management

Questions were posed to ascertain the level of identification of risks and vulnerabilities and the application of administrative actions to ensure the County Government's ICT infrastructure is adequately protected. Respondents were asked if there existed any metrics used to measure Cyber incident response capabilities at the county level. The majority of respondents at 69% said there were no metrics used to measure Cybersecurity at the county level, 8% said yes while 23% were not sure. When asked if cyber incident risk assessments were performed periodically at the county level, 73.1% said yes, 15.4% said no while 11.5% were not sure. The respondents were also asked about threat management programs put in place by the county government. The majority of the respondents at 40% did not believe the county had such programs, 32% of the respondents believed the county had implemented such programs while 28% were not sure. Consequently, those who believed the county had threat management programs, were asked how often the threat management programs were reviewed. A majority at 77.8% of the respondents

said there was no set period for review and update of the plan while 22% believed the programs were reviewed annually.

To establish the existence of a Cybersecurity incident response plan (CSIRP), the respondents were asked to describe the CSIRP in their departments. The majority of respondents at 76.9% said the county's Cybersecurity incident response plan (CSIRP) was 'ad hoc.' 11.5% of the respondents said they did not have a CSIRP. 7.7% of the respondent said they had CSIRP but it was not applied across all the county departments while 3.8% mentioned there was a CSIRP applied across the county departments. This is shown in *Figure 4.5* below.

Figure 4.5 A pie chart of the existence of a Cybersecurity incident response plan (CSIRP).

Consequently, the respondents were asked how often the CSIRP was reviewed. A majority at 60.9% said there was no set time period for review and update of the plan while 39.1% said the plan had never been reviewed or updated since its adoption.

Respondents were asked whether they were aware of the existence of the IT Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). A majority of the respondents said the county had either a business continuity plan (BCP) or disaster recovery plan (DRP) at 84.6%, 11.5%

were not sure while 3.8% believed no such plans existed at the county. Subsequently, the respondents were asked how often the DRP or BCP was reviewed. The majority of the respondents said there were no set periods for review and update of the plans at 75%. This was followed by 8.3% of respondents who said the plan has never been reviewed or updated since its adoption. This is shown in *Figure 4.6* below.

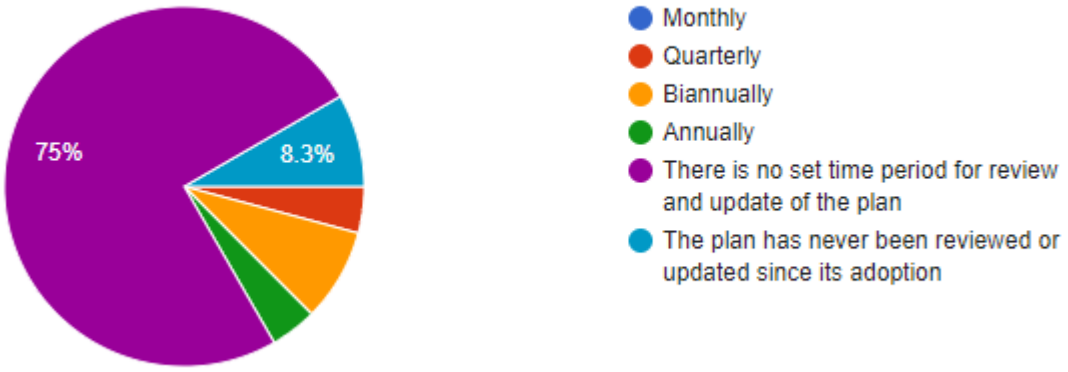

Figure 4.6 A pie chart of review of DRP/BCP.

4.2.5.3 Resources

Questions were fielded to the respondents to assess the availability of resources that ensure effective cyber incident response capabilities. The respondents were asked about the existence of tools and infrastructure for supervising information security at the county level. From *Figure 4.7* below, 53.8% of respondents affirmed the county had tools and infrastructure (e.g. anti-virus, firewalls) that monitor its security parameters. 23.1% of the respondents said no while another 23.1% were not sure.

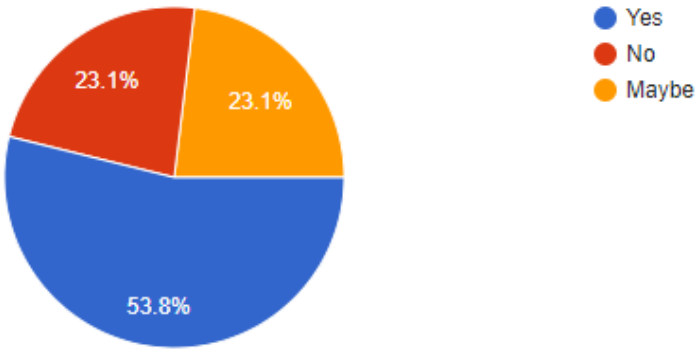

Figure 4.7: A pie-chart of response on the existence of tools and infrastructure for monitoring security

Subsequently, the respondents were asked whether the tools and infrastructure that monitor security parameters in the county were effective. 55% of the respondents were not sure while 30% disagreed. Only 5% of the respondents said the tools and infrastructure were effective. This is shown in *Figure 4.8* below.

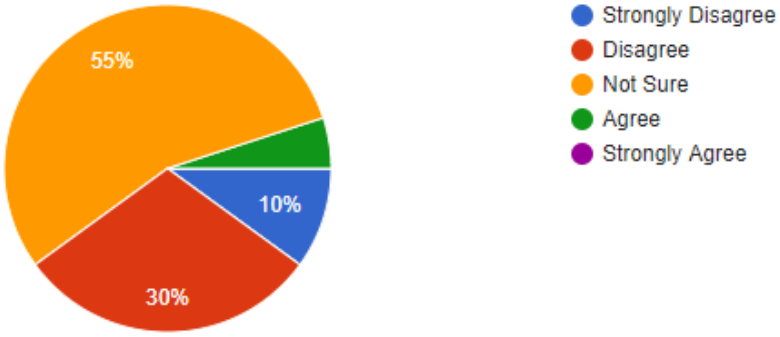

Figure 4.8: A pie-chart of response on whether the tools and infrastructure are effective.

The respondents were asked if they had antivirus installed on their computers and how often the antivirus was updated. A majority at 66.7% said they had antivirus installed on their computer even though a majority of them at 72% were not sure how often or if at all the antivirus

softwares was updated. The respondents were also asked if they believed the County Government allocated enough financial resources to cybersecurity measures. 76.9% of respondents did not believe so while only 3.8% said the county had allocated adequate financial resources on cybersecurity measures. Consequently, 61.5% and 38.5% strongly agreed and agreed respectively that the county should increase its budget for cybersecurity measures. Lastly, the respondents were questioned on the level of collaboration on cybersecurity knowledge sharing by the county government's ICT team. 69.2% of the respondents who responded to the question were not sure, 23.1% said no, while only 7.7% said yes.

4.2.5.4 Training

Questions were fielded to the respondents to assess the presence and their attendance of cybersecurity awareness programs that inform them of the actions to take to reduce the county's cybersecurity issues. The respondents were asked if end-user training on cyber incident response was done for all employees, either as part of general training or specifically on the topic of computer security and company policy.

As indicated in *Figure 4.9* below, 58.3% of the respondents said the cybersecurity and awareness training was done annually, 20.8% said the county had not conducted Cybersecurity awareness and training, 8.3% of the respondents said there were biannual cybersecurity training while 4.2% said there were quarterly.

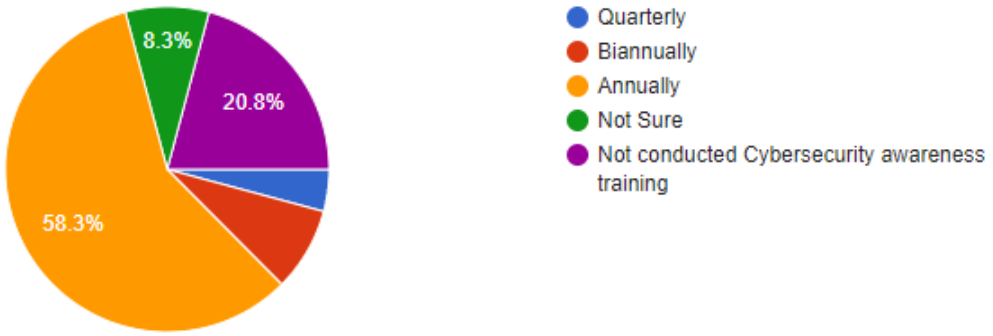

Figure 4.9: A pie chart of the frequency of cybersecurity incident training and awareness.

When asked if they had attended or received cybersecurity awareness training, 69.4% said they had never attended cybersecurity awareness training, 12.2% said they twice while 8.2% said they either attended once or quarterly. This is shown in *Figure 4.10* below.

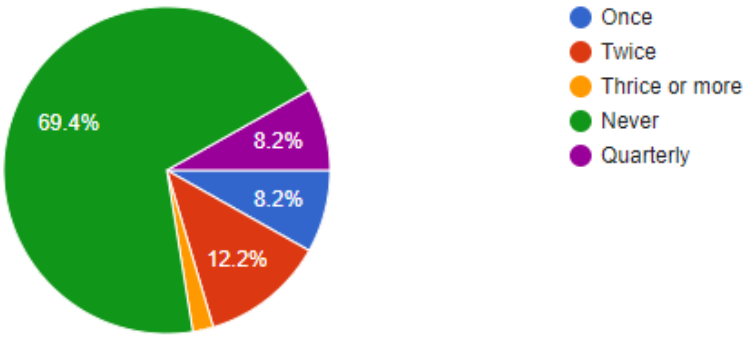

Figure 4.10: A pie-chart of cybersecurity incident training and awareness attendance annually.

The respondents were also asked about the frequency of practising responding to mock cyber incidents. 50% of the respondents indicated they practised at least once a year while 38.5% said they practised twice.

4.2.6 Ordinal Regression

The *Spearman's* rank-order correlation coefficient

Spearman's rank-order correlation coefficient (ρ, also signified by r_s) was used to establish the correlation matrix between the four independent variables and the cyber incident response capability variable. It was appropriate since the research collected nonparametric data. It measured the direction and strength of association between the four independent variables; policies, training, risk management approaches, and resources, and the dependent variable effective cyber incident response. The results are shown in *Table 4.2* below.

Table 4 2: Correlation matrix between Cyber incident response capabilities variables

Correlations			
			Effective Cyber Incident Response
Spearman's rho	Policies	Correlation Coefficient	.433
		Sig. (2-tailed)	.000
		N	76
	Training	Correlation Coefficient	.196
		Sig. (2-tailed)	.090
		N	76
	RiskManagementApproaches	Correlation Coefficient	.339
		Sig. (2-tailed)	.003
		N	76
	Resources	Correlation Coefficient	.287
		Sig. (2-tailed)	.012
		N	76
	Cyber Incident Response Effectiveness	Correlation Coefficient	1.000**
		Sig. (2-tailed)	.
		N	76

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

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

Table 4 3: Model Fitting Information

Model Fitting Information				
Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	147.773			
Final	91.041	56.732	16	.000

Null hypothesis: There is no significant difference between the Baseline Model to Final Model. From *Table 4.3* above, the significant value $\alpha=0.000<0.05$ rejects the null hypothesis. This affirms the existence of a significant difference between the Baseline Model to Final Model.

Table 4 4: Goodness of Fit

Goodness-of-Fit			
	Chi-Square	df	Sig.
Pearson	120.266	128	.674
Deviance	89.655	128	.996

The Pearson's significant value in *Table 4.4* above is 0.674 which is greater than 0.05. This proves that the observed data is having a goodness of fit with the fitted model.

Table 4 5: Pseudo R-Square

Pseudo R-Square	
Cox and Snell	.526
Nagelkerke	.612
McFadden	.380

From *Table 4.5*, the Cox and Snell value show that 52.6% in the variation of the dependent variable (effective cyber incident response capability) can be explained by a unit increase in policies, risk management, resources, and training.

Table 4 6: Parameters Estimates

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Location	[Policies=1]	-4.141	1.189	12.142	1	.000	-6.471	-1.812
	[Policies=2]	-4.131	1.384	8.912	1	.003	-6.843	-1.419
	[Policies=3]	-1.259	.969	1.687	1	.194	-3.158	.640
	[Policies=4]	-1.041	.980	1.127	1	.288	-2.963	.881
	[Policies=5]	0[a]			0			
	[Training=1]	-2.313	1.087	4.525	1	.033	-4.444	-.182
	[Training=2]	-1.955	1.123	3.029	1	.082	-4.156	.246
	[Training=3]	-.732	.906	.653	1	.419	-2.508	1.044
	[Training=4]	.179	.953	.035	1	.851	-1.688	2.047
	[Training=5]	0[a]			0			
	[Risk Management =1]	-1.959	1.268	2.389	1	.122	-4.444	.525
	[Risk Management =2]	-2.457	.918	7.163	1	.007	-4.256	-.658
	[Risk Management =3]	-2.174	.969	5.027	1	.025	-4.074	-.274
	[Risk Management =4]	.839	.826	1.033	1	.309	-.779	2.458
	[Risk Management =5]	0[a]			0			
	[Resources=1]	-2.410	.964	6.254	1	.012	-4.298	-.521
	[Resources=2]	-2.522	.985	6.560	1	.010	-4.452	-.592
	[Resources=3]	-1.326	.939	1.994	1	.158	-3.168	.515
	[Resources=4]	-.136	.857	.025	1	.874	-1.816	1.544
	[Resources=5]	0[a]			0			

Table 4 7: Test of Parallel Lines

Test of Parallel Lines[a]				
Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	91.041			
General	65.104[b]	25.937[c]	16	.055

The null hypothesis states that the location parameters (slope coefficients) are the same across response categories.[a]

a. Link function: Logit.

b. The log-likelihood value cannot be further increased after maximum number of step-halving.

c. The Chi-Square statistic is computed based on the log-likelihood value of the last iteration of the general model. The validity of the test is uncertain.

The significance value in *Table 4.7* $\rho = 0.055 > 0.05$ hence the null hypothesis is not rejected.

4.3 Tests of Hypotheses

Null Hypothesis: $H0_1$ Policy factors do not have an effect on effective cyber incident response capabilities at the county level.

Alternate Hypothesis HA_1 Policy factors affect effective cyber incident response capabilities at the county level.

From *Table 4.2* above, it was found that policies had a moderate positive correlation with effective cyber incident response capability at 0.433 and were significant($\alpha=0.000 <0.05$) at a 95% confidence level. The null hypothesis is therefore rejected.

Null Hypothesis $H0_2$: Risk management factors do not have an effect on effective cyber incident response capabilities at the county level.

Alternate Hypothesis HA_2: Risk management factors affect effective cyber incident response capabilities at the county level

As seen in *Table 4.2.*, risk management had a moderate positive correlation coefficient with effective cyber incident response capabilities at 0.339. It was also significant at $\rho=0.03 <0.05$. The null hypothesis is therefore rejected.

Null Hypothesis $H0_3$:Resources factors do not have an effect on effective cyber incident response capabilities at the county level.

Alternate Hypothesis HA_3: Resources factors affect effective cyber incident response capabilities at the county level

Resources had a positive but low correlation with effective cyber incident response capability with a coefficient of 0.287 as seen in *Table 4.2* above. However, it was not statistically significant with $\rho=0.12>0.05$. The null hypothesis is therefore not rejected.

Null Hypothesis $H0_4$: Training factors do not have an effect on effective cyber incident response capabilities at the county level.

Alternate Hypothesis HA_4: Training factors affect effective cyber incident response capabilities at the county level

From *Table 4.2* above, training has a positive but weak correlation with effective cyber incident capability with an $r=0.196$. It was also statistically insignificant with $\rho=0.90>0.05$. Therefore the null hypothesis is not rejected.

4.4 Discussion

This section presents the discussion and makes arguments and counter-arguments from the data findings and analysis. The research sought to formulate a localized cyber incident response framework for county governments in Kenya. To achieve that, the research set to answer three key research questions to drive the objectives.

1. **What are the major cyber incidents faced by the County Government of Migori?**

From the findings, natural or manmade disasters and IT systems downtime are the major cyber incidents faced by the county government. These findings can be attributed to the frequent fire incidents that have been experienced in various county offices such as in Migori and Kisii in the year 2020, and Garissa and Kisumu Counties in 2021 (Igadwah, 2020: Matete, 2020; Matete, 2021). The findings were similar to that of Koech (2016) interruption of utility supply and unplanned IT and Telecomm outages were the highest threats to county governments. The volume and severity of these incidents have also increased in the past two years. Severity is the measure of the amount of damage or harm that can be caused by the identified cyber incidents. Volume measures the frequency and number of ICT infrastructures affected by the occurrence of the identified cyber incidents. The findings are in agreement with Kshetri (2019) who found that there were increasing cyberattacks in Africa owing to the high degree of digitization versus vulnerable systems and lax cybersecurity practices.

2. **What variables are necessary for evaluating the cyber incident response capabilities of county governments in Kenya?**

The research successfully collated four variables derived from prior frameworks and literature review while taking into consideration the research problem and objectives. Policies, risk

management, resources, and training were found to be the variables necessary to evaluate the cyber incident response capabilities at the count level. The variables from the definition of cybersecurity by ITU were combined with those from the Serianu cybersecurity framework, ISACA guidelines on IT Governance and Management, and The National KE-CIRT/CC Framework to arrive at the four variables which were used to create a local framework.

3. **What are the indicators for measuring effective cyber incident response capabilities by the county governments?**

Consequently, the research sought to determine the indicators for measuring effective cyber incident response capabilities by the county governments. The research determined the indicators specifically suited for County Governments of Kenya which face certain unique threats while taking into consideration the Kenyan legal framework as well as international standards and regulations. The indicators for the first variable, policies, were cyber security strategies, policies, and standards. The indicators for risk management were risk assessment, threat management programs, cybersecurity incident response plan (CSIRP), Disaster Recovery Plan (DRP), and Business Continuity Plan (BCP). The indicators for resources were budget/financing of Cyber security, tools and infrastructure, and collaborations on the cyber incident response by ICT staff. Lastly, the variable training was indicated by the existence of training and awareness and attendance rate.

4.4.1 Policy and Effective Cyber incident response capability

The first objective of the research was to investigate the influence of policy on effective cyber incident response capabilities at the county level. The study found that policies influence cyber incident response capability in that as policies increase, the county cyber incident response effectiveness also increases. This is an agreement with Waweru (2015) and ITU (2018) and on the importance of cyber security policies that build user awareness and empower organization employees to be able to identify cybersecurity problems. In this regard, the County Government of Migori has adopted both national and localized cybersecurity policies and implemented cybersecurity strategies aimed at addressing risks. The County Government ICT, for instance, has adopted Computer Misuse and Cybercrimes Act No. 5 of 2018 which is a requirement by the national government for its devolved ICT services. However, the staff knowledge and adherence to these policies and strategies are low presenting a weak cyber incident response capability at the county level. A majority of the county staff neither understand the cybersecurity policy nor believe the strategies are adequate in addressing the business risks. In a study on information security policy non-compliance, (McLeod & Dolezel, 2021), found that a majority of employees were unaware of their organization's IT policies and had little user compliance to protect computing resources. This is in agreement with the findings of this research in regards to awareness of Cybersecurity policy at the county level which was higher among IT staff compared to non-IT staff. Policies are as good as they are adhered to. While there is higher compliance with national legislation and policies at the county level, a similar level of adherence and compliance should be encouraged for the localized cybersecurity policies that address cyber incident response at the county level.

4.4.2 Risk management and effective cyber incident response capability

The second objective of this research was to investigate the influence of risk management on effective cyber incident response capability at the county level. The study established that risk management factors influenced cyber incident response capability at the county level. The study found that while risk assessments were conducted frequently at the county, the majority of staff were not aware of the metrics used to measure cyber incident response capabilities at the county level. The absence of such measures could lead to a false sense of cyber incident response readiness at the county level. A similar lack of awareness exists when it comes to comprehensive threat management programs at the county level. A majority of county staff are not aware of such programs and how often they are reviewed or updated. The county government also relies on an ad hoc Cybersecurity incident response plan (CSIRP). The danger of such a plan is there is no way to review its suitability since it is unplanned. The county government is therefore at risk of ineffective cyber incident response in case of a cyber-incident that has never been factored into the plan. The county government has a business continuity plan (BCP) or disaster recovery plan (DRP). However, there are no set periods for review and update of the plan according to a majority of staff. This represents a weakness in ensuring effective cyber incident response at the county level. Koech (2016) found that risk management and Business Impact Analysis were fairly undertaken at the county level which agrees with this study's findings. Performing frequent risk analysis and assessments help determine appropriate countermeasures that can be put in place to ensure an effective response to some of the major identified cyber incidents at the county level.

4.4.3 Resources and effective cyber incident response capability

The third objective of this research was to investigate the influence of resources on effective cyber incident response capability at the county level. In this study, resources factors did not have an effect on effective cyber incident response capabilities at the county level. The county government has availed tools and infrastructure such as anti-virus and firewalls to its employees to increase their level of protection against cyber threats. However, the majority of county staff are not aware of how often or if not their anti-virus softwares are updated which poses a risk in case of cyber-attacks on their workstations. From the study, the county government had an inadequate budget allocation to cybersecurity measures. The findings were in agreement with Wechuli et al (2014) where they noted that while a majority of IT experts in the ministry of education had the knowledge required, they could not implement effective cybersecurity measures without sufficient funding. While this study found that resources did not influence cyber incident response capability, other studies such as Mayunga (2019) found that an organization requires adequate resources that can handle sustained attacks to successfully mitigate and thwart cyber attacks.

4.4.4 Training and effective cyber incident response capability

The fourth objective of this research was to investigate the influence of cybersecurity training on effective incident response capability at the county level. While studies such as by (Aldawood & Skinner, 2019) found cybersecurity awareness training influenced the cybersecurity state of organizations and therefore cyber readiness and response, in this study, training was found to have an insignificant effect on cyber incident response capability. The finding is in line with (McCrohan et al., 2010) who found that training had little or no influence on the change of human cybersecurity behaviour, especially among low-level employees. This is not to underscore the value of training in ensuring a safe ICT operating environment. However, the majority of the county staff place

higher importance on factors like policies and risk management as more important in ensuring effective cyber incident response capability at the county level. While the county requires employees to undergo cyber awareness and training, there is inadequate follow up hence the majority of staff never attend such events.

4.4.5 Proposed Cyber Incident Response Capability Framework

The primary objective of the research was to formulate a framework for effective cyber incident response capability at the county level. From the data collection and analysis, the research established each of the identified independent factors to the existence of total effective cyber incident response capability at the county level. The correlation analysis carried out led to the development of the proposed cyber incident response framework shown in *Figure 4.11* below. From the research findings, the county staff indicated they placed a high value on policies, risk management, resources, and training.

From the data collection and analysis, it was found that policies had the highest correlation with effective Cybersecurity incidence response capabilities at the county level while training had the lowest. This was in line with the finding that there was a lack of adequate Cybersecurity awareness by the county staff especially the end-users respondents. This means that even with adequate policies or funding, without consequent Cybersecurity awareness and training of end-users and IT staff, the county will still be ineffective in responding to any Cybersecurity incident. Risk management was the second most important construct according to the correlation coefficients. This highlights the importance of the county investing in risk management approaches that promote effective Cyber incident responses.

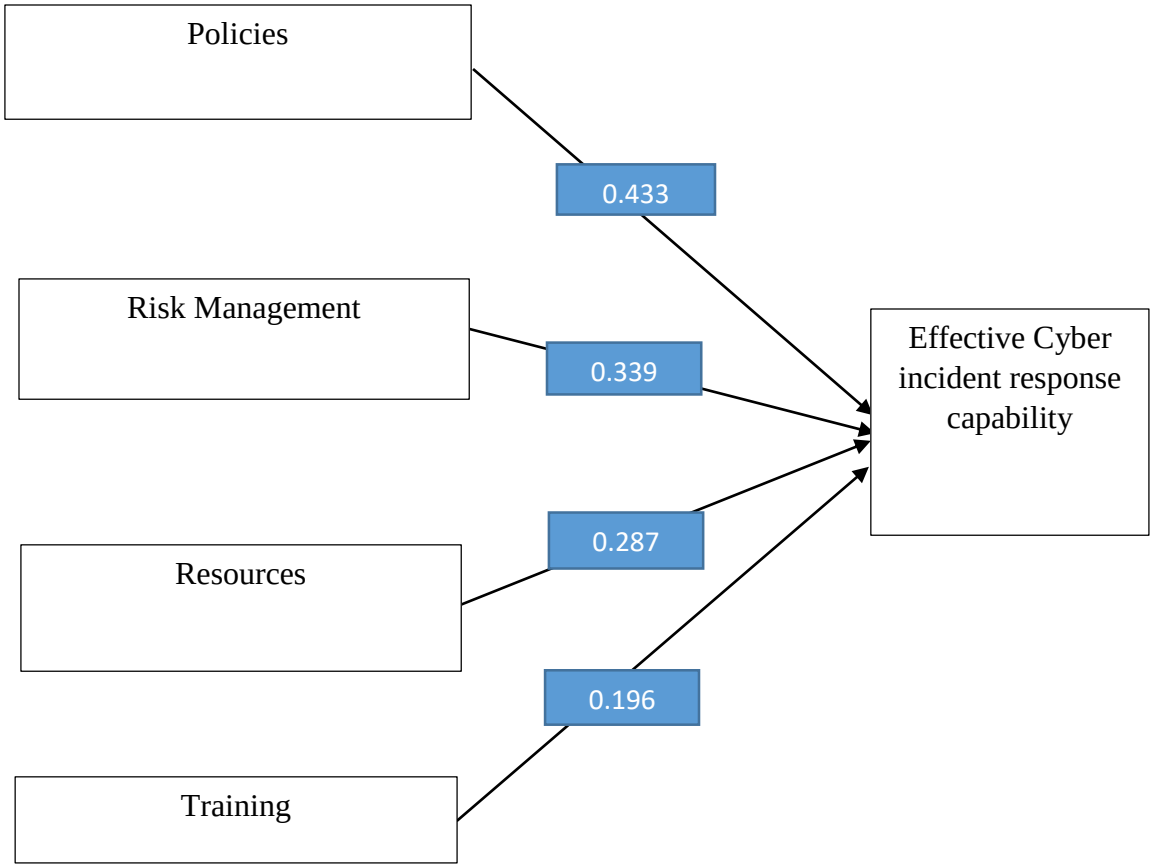

Figure 4.11 Proposed Cyber incident response capability framework for Migori County.

4.5 Summary of Findings

The key takeaway from this research is that the volume and severity of cyber threats have increased over the past years at the county level and in the absence of a localized cyber incident response framework, the county government is at risk of severe ICT service disruptions in case of a major cyber incident. The research has therefore successfully developed a localized cyber incident response capability framework for ensuring effective cyber incident response at the county level as shown in *Figure 4.11*. The research has also established that all the four independent variables; policies, risk management, resources, and training had positive correlations with effective cyber incident response capability. However, resources and training were insignificant. Policies had the highest correlation coefficient while training had the lowest. This shows the higher sense of importance placed on cyber security policies by the county staff. While the county had put in place some cybersecurity policies, standards, and strategies for addressing business risks, compliance with such was still low amongst the county staff especially in regards to local policies and legislations.

5 CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This section presents the conclusions and recommendations based on the objectives of the research. It also gives areas of further research in regards to effective cyber incident response capability at the county level.

5.2 Conclusion

The primary objective of this research was to develop a localized cyber incident response framework for cyber incident response at the county level. The study through an extensive literature review of existing cybersecurity frameworks and models identified four constructs and their indicators that befitted as key factors that influence effective cyber incident response capability at the county level. Consequently, the study adopted descriptive approaches augmented by quantitative techniques to measure the variables and find the influence of the four variables namely policies, risk management, resources, and training on the independent variable effective cyber incident response capability at the county level. The research conducted an online survey and collected data from 76 respondents within the county from which the four constructs were measured.

The research sought Spearman's rank-order coefficient correlation of the four constructs with effective cyber incident response capabilities. The study found that all the four independent constructs; policies, risk management, resources, and training, had a positive correlation coefficient with the dependent variable effective cyber incident response capability, however, the resources and training were found to be insignificant.

The correlation coefficients informed the development of the localized cyber incident response framework fulfilling the study's primary objective. From the findings of the study, the cyber incident response capability model developed explains 52.6% of cyber incident response capability by the county government.

5.3 Recommendations

Technology is dynamic hence efficient Cybersecurity incidence response capability is not a destination, it changes with the increased adoption of technology which comes with new cyber threats and exposures. However, at its current state, the county of Migori is weak in its Cybersecurity response capabilities and calls for more investments in the constructs which have been identified in this research. Most importantly, there should be increased implementation and compliance to policies, strategies, standards, and legislation at the county level. Secondly, the county should adopt risk management approaches including frequent risk assessments and threat management programs. These programs have to be reviewed and updated at least twice annually to ensure that they are at par with the technological developments and ICT services at the county level. The findings of this research do not underscore the value of resources and cyber awareness and training as factors in effective cyber incident response in as much as they were found to be insignificant. The county ICT staff must continue communicating cybersecurity requirements and appropriate behaviour through programs aimed at providing training on the ethical, protective, and lawful use of the county's ICT resources.

5.4 Future Studies

This research identified and focused on four constructs; policies, training, risk management, and resources as major factors in effective cyber incident response capability at the county level. However, due to time and resource constraints, the developed framework was not validated at the county level. Future research should validate the viability of the framework and also improve on more variables that are likely to affect cyber incident response capability as the adoption of ICT services increases at the county level.

6 References

Abomhara, M., & Koien, G. M. (2014). Cyber security and the internet of things: Vulnerabilities, threats, intruders, and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414 (Accessed April 2021).

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073 (Accessed September 2021).

African Union. (2016). (working paper). *Page 1of 10A global approach on Cybersecurity and Cybercrime in Africa* (pp. 1–10).

Allen, N. (2021). *Africa's Evolving Cyber Threats*. Africa Center for Strategic Studies. https://africacenter.org/spotlight/africa-evolving-cyber-threats/. (Accessed April 2021).

Antonucci, D. (2017). *Cyber Risk Handbook: Creating and measuring effective cybersecurity capabilities*. New Jersey: John Wiley & Sons.

Awuor, O. M., Agalo, J., & Day, P. (2018). Gender influence in communication for development: A study of Migori county government, Kenya. *International Journal of Innovative Research and Development*, *7*(6), 229–239. https://doi.org/10.24940/ijird/2018/v7/i6/jun18121 (Accessed July 2021).

Chitechi, V. K., Mbugua, S., & Omieno, K. (2018). Facilitating Factors for Cybersecurity Vulnerabilities in Kenyan County Governments. *Asian Journal of Research in Computer Science*, *2*(1), 1-11. https://doi.org/10.9734/ajrcos/2018/v2i124773 (Accessed April 2021).

Chitehi, K. V., Kimeo, K. K., & Mbugua, S. (2021). Cyber-Security Vulnerability Assessment Model for County Governments in Kenya. *International Journal of Science and Research (IJSR)*, *10*(7), 792–797. https://doi.org/10.21275/SR21714030154 (Accessed April 2021).

Communications Authority of Kenya. (2020). (rep.). *SECOND QUARTER CYBERSECURITY SECTOR STATISTICS REPORT FOR THE FINANCIAL YEAR 2019/2020(OCTOBER-DECEMBER2019)* (pp. 1–26). Nairobi: Kenya Government Press.

Durga, M. S., Nayak, P., & Narayak, K. A. (2019). Strengths and weaknesses of online surveys. *IOSR Journal of Humanities and Social Sciences (IOSR-JHSS)*, *24*(5), 31–38. https://www.researchgate.net/profile/Mudavath-Nayak/publication/333207786_Strengths_and_Weakness_of_Online_Surveys/links/61176e5a0c2bfa282a42253b/Strengths-and-Weakness-of-Online-Surveys.pdf (Accessed June 2021).

Hove, C., Tarnes, M., Line, M. B., & Bernsmed, K. (2014). Information security incident management: Identified practice in large organizations. *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*. https://doi.org/10.1109/imf.2014.9 (Accessed March 2021)

Igadwah, L. (2020, December 21). *Fire leaves Migori without SH1.5BN receipts, says Ouko*. Business Daily. Retrieved September 15, 2021, from

https://www.businessdailyafrica.com/bd/economy/fire-leaves-migori-without-sh1-5bn-receipts-says-ouko-2243880 (Accessed September 2021).

Information Systems Audit and Control Association (ISACA). (2020). (rep.). *State of Cybersecurity 2020: Part 2: Threat Landscape and Security Practices* (pp. 1–23).

International Telecommunication Union (2004). Understanding Cybercrime: A Guide for Developing Country.

International Telecommunication Union (ITU). (2018). (publication). *Global Cybersecurity Index (GCI) 2018* (pp. 1–92). London, UK: International Telecommunication Union (ITU).

ISO/IEC 27000. (2018). *Iso/IEC 27000:2018*

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, *7*(4), 396–403. https://doi.org/10.9734/bjast/2015/14975 (Accessed July 2021).

Kiboi, B. N., & Kiboi, B. N. (2015). *Cyber Security as an emerging threat to Kenya's national security* (dissertation). University of Pretoria, Pretoria. Retrieved from https://repository.up.ac.za/bitstream/handle/2263/50644/Kiboi_Cyber_2015.pdf?sequence=1&isAllowed=y (Accessed October 2020).

Kleinberg, H., Reinicke, B, Cummings, J., Tagliarini, G. (2015) Building a Theoretical Basis for Cyber Security Best Practices. Annals of the Master of Science in Computer Science and Information Systems at UNC Wilmington, 9(2) paper 12. http://csbapp.uncw.edu/data/mscsis/full.aspx. (Accessed April 2021).

Koech, B. K. (2016). *Evaluation Framework For It Service Continuity And Disaster Recovery Plans: The Case In Kenya'S County Governments.* (thesis). University of Nairobi, Nairobi.

Kothari, C. R., & Garg, G. (2004). *Research Methodology: Methods and techniques* (2nd ed.). New Delhi: New Age International (P) Limited.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198x.2019.1603527 (Accessed September 2021).

Kumar, R.(2011). Research Methodology: A step-by-step guide for beginners. (3rd Edition). London: Sage Publications

Matete, F. (2020, September 4). *Property worth Millions destroyed as FIRE razes KISII county assembly*. The Star. Retrieved September 10, 2021, from https://www.the-star.co.ke/counties/nyanza/2020-09-04-property-worth-millions-destroyed-as-fire-razes-kisii-county-assembly/. (Accessed September 2021).

Matete, F. (2021, September 6). *Arson suspected as section Of Kisumu county OFFICES razed*. The Star. Retrieved September 15, 2021, from https://www.the-star.co.ke/counties/nyanza/2021-09-06-arson-suspected-as-section-of-kisumu-county-offices-razed/ (Accessed September 2021).

Matinde, V. (2014). *Kenya's government unveils cyber security strategy*. ITWeb Africa. https://itweb.africa/content/lLn14MmjD2QqJ6Aa (accessed April 24, 2021)

Mayunga, M. O. (2019). *Developing And Assessing A Cyber-Resilience Framework For Kenyan Banks.* (thesis). Africa Nazarene University, Nairobi.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415 (Accessed September 2021).

McAfee. (2021). *How Cybersecurity Policies and Procedures Protect Against Cyberattacks*. McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html. (Accessed August 2021).

McLeod, A., & Dolezel, D. (2021). Information security policy non-compliance: Can capitulation theory explain user behaviours? *Computers & Security*, 102526. https://doi.org/10.1016/j.cose.2021.102526 (Accessed September 2021).

Migori County Government. (2021). *The official website of the migori county government*. Migori County Website. https://migori.go.ke/. (Accessed September 2021).

Migori County. (2018). (rep.). *MIGORI COUNTY DRAFT ANNUAL PROGRESS REPORT* (pp. 1–42).

Ministry of Information Communication and Technology. (2014). *The Kenya National ICT Masterplan 2014-2017*. Government of Kenya.

Mugenda, O. M., & Mugenda O. M. (2003). Research methods. *Quantitative and Qualitative Approaches.*

Muhati, E. (2018). Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises (Thesis). Strathmore University. Retrieved from http://su-plus.strathmore.edu/handle/11071/6013 (Accessed September 2021).

Muthaura, M. S., Ayugi, C., & Amondi, A. (2018). (publication). *Getting the Deal Through - Pensions Retirement Plans 2018* (pp. 1–42). London: Law Business Research Ltd.

Republic of Kenya (ROK)(2010), The Constitution of Kenya, Nairobi.

Serianu. (2015). *Kenya Cybersecurity Report 2015: Cyber Crime & Cybersecurity trends in Africa*. Retrieved April 2, 2021, from http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf (Accessed May 2021).

Serianu. (2017). *Kenya Cybersecurity Report 2017*. Retrieved from https://www.serianu.com/downloads/KenyaCyberSecurityReport2017.pdf (Accessed May 2021).

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: A flexible approach. *Computer Fraud & Security*, *2021*(1), 14–19. https://doi.org/10.1016/s1361-3723(21)00009- (Accessed March 2021).

Thompson, L. N. (2019). *Cybersecurity Best Practices for Municipalities*. New Hampshire Municipal Association. https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities. (Accessed March 2021).

Tödtling , T., Eysin, U., & Bosire , C. (2018). (rep.). *Devolution in Kenya: Driving forces and future scenarios* (pp. 1–132). Nairobi: Strathmore University Press.

Walt, S. (1998). International Relations: One World, Many Theories. *Foreign Policy,* (110), 29-46. doi:10.2307/1149275

Waweru, R. (2019). *Cyber Security Readiness Assessment Model In Kenyas' Higher Learning Institutions: A Case Of University Of Nairobi* (thesis). University Of Nairobi, Nairobi.

Wechuli, A. N., Muketha, G. M., & Matoke, N. (2014). Survey of Cyber Security Frameworks. International Journal of Technology in Computer Science & Engineering. *International Journal of Technology in Computer Science & Engineering*, *1*(2), 33–39.

Yamane, T. (1973) Statistics: An Introductory Analysis. 3rd Edition, Harper and Row, New York.

7 APPENDICES

7.1 Appendix 1A: Questionnaire: Cyber Incident Response Capabilities in Migori County.

This is a questionnaire seeking to determine the cyber incident response capabilities in Migori County. This study is purely for Academic purposes and all responses will be kept strictly confidential. The questionnaire is divided into 7 parts. When completing the questionnaire, you can leave blank any questions that you do not want to answer or you feel do not apply to you. Please try to answer all the questions.

Part 1: Demographic Information

1) Gender
   - Female
   - Male
2) Age
   - 18-24
   - 25-34
   - 35-44
   - 45-54
   - Over 55

3) What is your job title?

   ……

4) Which County Department best describes your roles and responsibilities?
    - Public Service and Administration
    - Information Communications Technology-ICT
    - Health Services
    - Finance and Economic Planning
    - Trade, Tourism, and Co-operatives
    - Agriculture, Livestock, Fisheries, and Water Development
    - Lands, Housing, and Physical Planning
    - Environment, Natural Resources, and Disaster Management
    - Roads, Transport, Public Works, and Energy
    - Education, Youth, Sports, Cultural, and Social Services

5) What is your highest level of education?
    - Certificate
    - Diploma
    - Degree
    - Masters
    - PhD

Part 2: Cyber Incidents Landscape at the County Level.

To what extent would you rate each of the following cyber incidents as threats to Cybersecurity at the county?

	Use a scale of 1-5 where, 1= no extent, 2= little extent, 3= moderate extent, 4= large extent, and 5= very large extent.				
Cyber incident	**1**	**2**	**3**	**4**	**5**
6) Hacking	○	○	○	○	○
7) It Systems Failure	○	○	○	○	○
8) Ransomware	○	○	○	○	○
9) Virus	○	○	○	○	○
10) Advanced Persistent Threat	○	○	○	○	○
11) Natural and Manmade Disasters	○	○	○	○	○
12) Disgruntled Employees	○	○	○	○	○
13) Human error	○	○	○	○	○

14) In the past two years, has the volume of the cyber incidents identified above increased in the county?

- ○ Yes
- ○ No
- ○ Maybe

15) In the past two years, has the severity of the cyber incidents identified above increased in the county?

- o Yes
- o No
- o Maybe

On a scale of 1-5, please rank the following items. 1=low 5=high					
	1	**2**	**3**	**4**	**5**
16) The county government's Cyber incident response capabilities	○	○	○	○	○
17) The county government's ability to prevent a cyber attack	○	○	○	○	○
18) The county government's ability to detect a cyber attack	○	○	○	○	○
19) The county government's ability to contain a cyber attack	○	○	○	○	○
20) The county government's ability to respond to cyber attack	○	○	○	○	○
21) The county government's ability to hire and retain cybersecurity personnel.	○	○	○	○	○

Part 3: Policies

22) a. Does the county have a Cybersecurity policy?

- o Yes
- o No
- o Maybe

b. If the answer to the above is yes, do you understand the county's Cybersecurity policy?

- Yes
- No
- Maybe

23) a. Does the county have a Cybersecurity strategy aimed at addressing business risks?

- Yes
- No
- Maybe

b. If the answer to the above is yes, do you agree that the county government's Cybersecurity strategy is effective in addressing business risk?

- Yes
- No
- Maybe

24) a. Is any of the listed Cybersecurity certification/standardization legislation or regulation adopted by the county government of Migori?

□ ISO 27001 (The international standard for information security)

□ ISO/IEC 27032 (Cybersecurity' or 'Cyberspace security)

□ ISO 22301:2019 (Security and resilience – Business continuity management systems - Requirements)

□ National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)

□ COMPUTER MISUSE AND CYBERCRIMES ACT. NO. 5 OF 2018

□ None

□ Other ……..

b. On a scale of 1 to 5, where 1 is low and 5 is high, how do you rate the compliance to the above ticked or mentioned standardization/certification(s) at the county level?

1	2	3	4	5
○	○	○	○	○

25) What do you think are the barriers to adopting and implementing national or international Cyber incident response frameworks or strategies at the county level?

□ Insufficient funding

□ Inability to hire and retain skilled Cybersecurity personnel

□ Lack of training for IT security staff

□ Lack of training of end-users

□ Lack of political goodwill and support from county leadership

□ Other …….

Part 4: Risk Management Approaches

26) Are there any metrics used to measure Cyber incident response capabilities at the county level?

- Yes
- No
- Maybe

27) Are cyber incident risk assessments performed periodically at the county level?

- Yes
- No
- Maybe

28) a. Has the county implemented threat management programs such as alerts based on intrusions?

- Yes
- No
- Maybe

b. If the answer to the above is yes, how often is the threat management program reviewed and updated?

- Monthly
- Quarterly
- Biannually
- Annually
- There is no set time period for review and update of the plan

29) a) Which of the statement best describes your department's Cybersecurity incident response plan (CSIRP)

- We have CSIRP and it is applied across the county departments
- We have CSIRP but it is not applied across all the county departments
- The county's CSIRP is "ad hoc"
- We do not have CSIRP

b) If you have a CSIRP, how often is it reviewed and tested?

- Monthly
- Quarterly
- Biannually
- Annually
- There is no set time period for review and update of the plan
- The plan has never been reviewed or updated since its adoption

30) a. Do you have a Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)?

- Yes
- No

b. If the answer to the above is yes, how often is the DRP or BCP reviewed?

- Monthly
- Quarterly
- Biannually
- Annually
- There is no set time period for review and update of the plan
- The plan has never been reviewed or updated since its adoption

Part 5: Resources

31) a. Does the county government have tools and infrastructure (e.g. anti-virus, firewalls) that monitor its security parameters on a regular if not real-time basis?

- Yes
- No
- Maybe

b. If the answer to the above is yes, do you agree that the tools and infrastructure that monitor security parameters in the county are effective?

- Strongly Disagree
- Disagree
- Not Sure
- Agree
- Strongly Agree

32) a. Does the computer you use for work have anti-virus?

- Yes
- No
- Maybe

b. If the answer to the above is yes, how often is the anti-virus program updated?

- Daily
- Weekly
- Monthly
- Not Sure
- Never

33) Does the county allocate adequate financial resources to cyber response measures?

- Yes
- No
- Maybe

34) The county government should increase its budget for Cybersecurity measures?

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

35) Does the county government's ICT team continually collaborate on Cybersecurity knowledge sharing practice?

- Yes
- No
- Maybe

Part 6: Training

36) a. Is end-user training on cyber incident response mandatory for all employees, either as part of general training or specifically on the topic of computer security and company policy?

- Yes
- No
- Maybe

b. If the answer to the above is yes, how frequent are the Cyber incident response awareness training conducted?

- Quarterly
- Biannually
- Annually
- Not Sure

37) Is there specialized cyber incident response training for personnel with IT or OT responsibilities?

- Yes
- No
- Maybe

38) Have you ever received training on cyber incident response or computer and information security?

- Yes
- No
- Maybe

39) How often do you rehearse mock incident responses and procedures needed to respond to cyber incidents?

- Once
- Twice
- Thrice or More
- Never

40) On a scale of 1 to 5, where 1 is low and 5 is high, how would you rate the effectiveness of the training in preparing you to respond to any cyber incident?

1	2	3	4	5
○	○	○	○	○

Part 7: Proposed Cyber Incident Response Capability Framework Constructs

41) **The following are 4 factors considered important in achieving effective Cyber incident response capabilities in Migori County. Please rank each factor in order of importance**

1-Most Important 5-Least Important

	1	2	3	4
Policies	○	○	○	○
Risk Management	○	○	○	○
Resources	○	○	○	○
Training	○	○	○	○
Effectiveness of Cyber Incident Response Capabilities	○	○	○	○

7.2 Appendix 1 B: Google Form Questionnaire URL Link

https://forms.gle/L763HU6o4BbiiHDV8