REPUBLIC OF KENYA

NATIONAL CRIME RESEARCH CENTRE

Fighting Crime through Research

INFORMATION COMMUNICATION TECHNOLOGY CRIMES AND OFFENCES IN KENYA

Kenneth Bundi Mbaya

Phyllis Muriuki

NATIONAL CRIME RESEARCH CENTRE

INFORMATION COMMUNICATION TECHNOLOGY CRIMES AND OFFENCES IN KENYA

COPYRIGHT

Nairobi; Printed in Kenya

ISBN

FOREWORD

In an increasingly digital world, the emergence of Information and Communication Technology (ICT) has revolutionized how we live, work, and interact. The Internet and digital technologies have brought immense benefits to individuals, businesses, and governments, facilitating seamless communication, efficient transactions, and unprecedented access to information. However, along with these advancements, a new threat has emerged -cybercrime.

The pervasiveness of ICT crimes and offences presents a complex challenge to societies around the globe, including Kenya. As technology continues to evolve, so do the tactics of cybercriminals, making it imperative for us to stay ahead in our efforts to combat and mitigate these threats. To address this critical issue, comprehensive research, and analysis are essential to understand the nature and impact of cybercrimes on our nation.

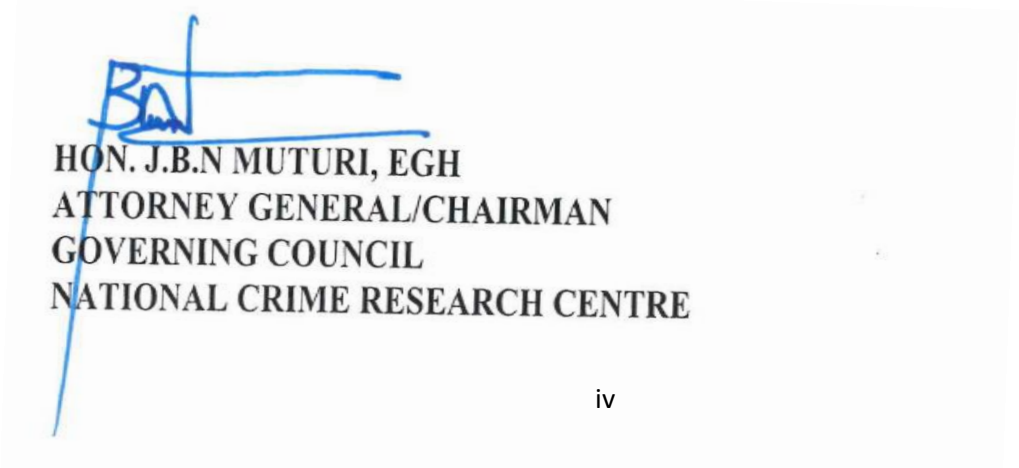
This study report comprehensively assesses the prevalence, characteristics, impacts, and challenges of ICT crimes and offences in Kenya. It examines the intricacies of cyber threats and the factors contributing to their proliferation and sheds light on the diverse forms of cybercrimes affecting different sectors and individuals in our society.

The study identifies the areas of vulnerability and also highlights the key players and institutions involved in combating cybercrimes. It outlines the challenges faced in addressing these threats and the level of satisfaction with the existing efforts to tackle cybercrimes.

The report provides several recommendations to guide policymakers, regulators, law enforcement agencies, and other stakeholders in formulating effective strategies to counter cyber threats. These recommendations include focused training, strategic collaborations, resource allocation and emphasis on data backups and evidence preservation.

I am confident that the findings and recommendations presented in this report will serve as a foundation for ongoing efforts to build a resilient and secure digital environment in our nation.

By working together we can create a safer cyber landscape for our citizens and empower our nation to thrive in the digital age.



HON. J.B.N MUTURI, EGH
ATTORNEY GENERAL/CHAIRMAN
GOVERNING COUNCIL
NATIONAL CRIME RESEARCH CENTRE

ACKNOWLEDGEMENTS

We extend our heartfelt gratitude to all the individuals and institutions that played a significant role in making this study possible. Without their unwavering support, dedication, and contributions, this comprehensive assessment of ICT crimes and offences in Kenya would not have been possible.

First and foremost, we express our deepest appreciation to the participants of this study. Your willingness to share valuable insights and experiences has been crucial in providing us with a comprehensive understanding of the prevalence and impacts of cybercrimes in our nation. Your cooperation and candid responses have been instrumental in shaping the findings and recommendations of this report.

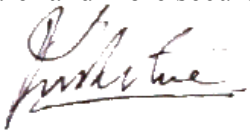
We would like to acknowledge the researchers and analysts involved in the data collection, processing, and analysis. Your tireless efforts and meticulous attention to detail have ensured the accuracy and reliability of the information presented in this study. Your commitment to excellence in research has contributed significantly to the quality of this report.

We are grateful to the institutions and organizations that supported and facilitated this study. Your willingness to collaborate and share data has been invaluable in conducting a comprehensive and holistic assessment of ICT crimes and offences in Kenya. Your dedication to addressing cyber threats and promoting a secure digital environment is commendable.

Special thanks go to the regulatory bodies, law enforcement agencies, and government institutions for their valuable insights and cooperation throughout the research process. Your expertise and guidance have provided valuable context and perspective, enhancing the relevance and applicability of our findings.

Lastly, we extend our appreciation to our peers, mentors, and colleagues who provided valuable feedback and support during this study. Your encouragement and constructive criticism have been vital in shaping the direction of our research.

In conclusion, this study would not have been possible without the collective effort and support of all the individuals and institutions mentioned above. We are deeply grateful for your contributions, and we hope that the insights and recommendations presented in this report will pave the way for a safer and more secure digital future in Kenya.



DR. MUTUMA RUTEERE (PhD)
DIRECTOR/CEO
NATIONAL CRIME RESEARCH CENTRE

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

CJS -	Criminal Justice System
COVID-19 -	Coronavirus Disease 2019
DCS -	Directorate of Children Services
ICTA -	Information and Communication Technology Authority
KE-CIRT -	Kenya Computer Incident Response Team Coordination Centre
KPS -	Kenya Prison Services
MICDE -	Ministry of Information, Communication, and Digital Economy
NC4 -	National Cybersecurity and Communications Integration Centre or similar
NPS -	National Police Service
ODPP -	Office of the Director of Public Prosecutions
SPSS-	Statistical Package for Social Sciences

EXECUTIVE SUMMARY

This executive summary presents the key findings, implications, and recommendations from a comprehensive study conducted to examine the prevalence, characteristics, impacts, and challenges of ICT crimes and offences in Kenya. The study aimed to gain insights into the nature of cybercrimes in the country and identify effective strategies to combat and mitigate their effects.

The study revealed that ICT crimes and offences are prevalent in Kenya, with various categories of cybercrimes affecting different sectors and individuals. A majority (67.5%) of respondents rated the prevalence as high, with 84.8% experiencing some form of ICT crime in the past 24 months. The most common crimes reported were computer fraud (72.9%), identity theft and impersonation (71.5%), and interception of electronic messages or money transfers (57.3%). These crimes have significant consequences, leading to financial loss, psychological distress, reputational damage, and even loss of life in extreme cases.

The study identified specific demographic trends among victims and perpetrators of cybercrimes. Offenders are predominantly youths (50.1%), ICT experts (43.9%), and inmates/prisoners (23.1%). Victims include the elderly (39.4%), the uninformed (28.2%), and major business players (21.0%). The financial sector is the most affected, followed by educational institutions and the telecommunication industry. Crimes such as online banking fraud, credit card scams, and phishing attacks are prevalent, highlighting the necessity for robust cybersecurity measures in these sectors.

The study found that the key contributing factors to these crimes include economic vulnerabilities like unemployment (87.8%) and poverty, psychological motives such as financial greed, and societal issues like lack of ICT literacy and misuse of advanced technology. ICT crimes have severe consequences, including significant financial losses (92.4%), psychological distress (68.6%), tangible property loss (60.1%), breaches of personal information (50.5%), and data loss (46.7%). These impacts necessitate urgent and multi-faceted interventions

The study also explored the role of institutions and agencies involved in addressing cybercrimes in Kenya. While efforts have been made by various entities, the level of satisfaction with their service delivery varied among respondents. There is a mixed level of satisfaction with institutional responses, with 47.1% of respondents expressing satisfaction and 52.9% indicating dissatisfaction.

Institutions like the Communication Authority and the National Intelligence Service received higher satisfaction ratings, while others like NC4 and ODPC had lower ratings. However, there were concerns regarding the effectiveness and coordination of measures taken to combat cyber threats.

The study found out the key measures in addressing ICT crimes include public awareness campaigns (74.4%), strong password emphasis (57.2%), controlled information sharing (46.7%), strict law enforcement (42.3%), and antivirus software use (41.4%). However, there is a need for improved data protection laws (31.3%) and controlled ICT infrastructure access (29.9%).

Several challenges were identified in tackling ICT crimes and offences in Kenya. Significant challenges include a lack of resources (23.9%), corruption within investigative bodies (20.5%), and a lack of public awareness (19.9%). Additional hurdles are the shortage of specialized ICT knowledge (17.9%), high levels of illiteracy (14.5%), and inefficiencies within the Criminal Justice System (13.4%) and poor enactment of the Computer Misuse and Cybercrime Act, 2019 policies further hindered the effective prosecution of cybercriminals.

Key Recommendations:

Recommendations: Based on the study findings, the following recommendations are proposed to address the challenges and strengthen efforts in combating ICT crimes and offences in Kenya:

1. **The need for regular Civic Education and Public Sensitization:** The Ministry of ICT and Launch public awareness and sensitization programs to educate citizens about various forms of cybercrimes and provide practical tips on how to protect themselves from cyber threats. Collaborate with relevant stakeholders, including schools, media, and community leaders, to amplify awareness.
2. **Strengthen Law Enforcement:** Ensure strict enforcement of cybersecurity laws and regulations. Establish specialized units within law enforcement agencies to handle cybercrime investigations and prosecutions. Invest in training and capacity building for law enforcement personnel to enhance their expertise in cybercrime investigation.

3. **Adequate Funding for ICT Regulatory Agencies:** Provide sufficient financial resources to ICT regulatory agencies to enhance their capabilities in preventing and responding to cyber threats. This includes investing in state-of-the-art technology and cybersecurity infrastructure.
4. **Collaboration Among Stakeholders:** Foster close collaboration among government agencies, private sector entities, civil society organizations, and international partners to develop a coordinated approach to tackling cybercrimes. Establish cybercrime response teams to facilitate information sharing and joint investigations.
5. **Cyber security Policy Review:** Conduct a comprehensive review of existing policies governing ICT to address the evolving dynamics of cyber threats. This should include updating and strengthening legislation to keep up with emerging cybercrime trends.
6. **Public Caution and Cyber Hygiene:** Encourage individuals and organizations to exercise caution while using technology and adopt strong cybersecurity measures, such as using strong and secure passwords, enabling two-factor authentication, and regular software updates.
7. **Strengthening the Criminal Justice System:** Address capacity and inefficiencies in the criminal justice system and accord more priority to cybercrime cases to ensure timely adjudication. Enhance collaboration between law enforcement agencies, prosecutors, and the judiciary to expedite the prosecution of cybercriminals.
8. **Investment in ICT Expertise:** Invest in building ICT expertise in various sectors through targeted training and capacity-building programs. This includes providing cybersecurity training for employees and ICT professionals.
9. **Research and Innovation:** Promote research and innovation in the field of cybersecurity to develop cutting-edge solutions and strategies to combat cybercrimes. Encourage collaboration between academia, industry, and government to address emerging cyber threats.

In conclusion, ICT crimes and offences pose significant challenges to individuals, businesses, and the overall security landscape of Kenya. The findings of this study underscore the urgent need for proactive measures to combat cyber threats effectively. By implementing the recommended strategies and fostering collaboration among stakeholders, Kenya can strengthen its cyber security ecosystem and create a safer digital environment for all citizens and entities.

CHAPTER ONE: INTRODUCTION

1.1. Background of the Study

The advent of technology has brought about both positive and negative effects on the world. The digital revolution has provided limitless opportunities such as easy access to information and global communication. However, it has also opened the door to various risks, making it easier for criminals to find unsuspecting victims and conduct crimes in cyberspace.

The term "cybercrime" encompasses a range of criminal activities involving the Internet, specific software, and other networked systems. These activities may intentionally or unintentionally cause harm to others or disrupt normal functioning, and they can be categorized as computer crimes, high-tech crimes, digital crimes, electronic crimes, or technology-enabled crimes. (Grabosky, 2017; Grabosky& Smith, 2017).

Globally, the incidence of ICT-related crimes has been increasing each year, making millions of people vulnerable. Cybercrime poses threats to public safety, economic stability, and national security. Perpetrators of cybercrimes are driven by various motivations, such as financial gain, emotional instability, cultural factors, and a lack of adequate laws and penalties.

Research on cybercrimes is still limited, and there is a pressing need to assess trends in cybersecurity. The study of cybercrime trends and patterns is particularly important for developing countries. By understanding these trends, such countries can strengthen their legal frameworks and enforcement efforts to prevent and combat cybercrimes effectively. (Ngo & Jaishankar, 2017).

1.1.1. Global Perspective

Cybercrimes have become a global problem. For instance, from 2006 to 2010 China had the highest reported crimes in Asia, followed by Taiwan, South Korea, and India. Vietnam is ranked 17th among 20 countries with the highest number of internet users in the world (Internet World Stats, 2018). In Vietnam, the most prominent computer-related crimes were hacking, and the focus was mainly on intrusions. For example, there was a case where 500 million dongs were extracted from a customer in 2018 (Symantec, 2018). In the Philippines, identity theft was the most dominant cybercrime as there was a record 258 cases in 2019, and in two years, reports of cybercrime increased with a record of 1.76 million reports of cybercrimes in the first three

months of 2021. There was an increase in child exploitation during the COVID-19 period since children started online classes and thus became vulnerable to cyber criminals online (Broadhurst & Yao-Chung Chang, 2012).

In the US, according to the US Internet Crime Complaints Centre, 2020 the three commonly reported cybercrimes based on complaints reporting were: phishing and pharming (32.96%), non-payment & non-delivery (14.87%), and extortion (10.48%). Phishing and pharming is the fraudulent practice of alluring people to reveal personal information, such as passwords, login details, and credit card numbers. Non-payment is where a buyer does not pay for received goods or services, while non-delivery is failure to deliver goods or services. The most common form of extortion was ransomware to access devices and files and then demand money payment according to the Centre.

In Europe, the country that is the most vulnerable to cybercrime is Malta, followed closely by Greece, Romania, and Slovakia. According to calculated cybercrime density, from 2020 to 2021, the United Kingdom had the highest density with 40%, the US (13%) and Canada (7%). The victims were mainly affected by phishing scams while investment fraud was the leading crime as it had a total loss of $1.5 billion. In Australia, 67,500 cyber-crimes reports were recorded, the dominant crimes recorded were exploitation and ransomware with a 15% increase between 2020 and 2021 (Surfshark, 2021).

Cybercrimes impact countries differently, and their costs are increasing rapidly due to technological growth and industrialization. For instance, in the US alone, the direct loss from internet crime was estimated to be around $559.7 million in a single year. (AFP, 2010).

1.1.2. African Perspective

Africa has the world's fastest-growing internet and phone networks and has a high-volume use of mobile banking services. Africa has about 500 million internet users which is, only 38 percent of the population and so offering huge potential for growth. Cybercrime affects all countries, but weak networks and security mean African countries are particularly vulnerable. This digital demand, coupled with a lack of cyber security policies and standards, exposes digital spaces to significant risks. African countries are moving towards entrenching digital infrastructure into all aspects of society including government, banks, businesses, and critical infrastructure, thus establishing a strong cybersecurity framework is critical (Kshetri, 2019).

East Africa has the quickest developing economies on the African landmass, it also has one of the quickest in the remainder of the world. There is an expansion of the computerized framework, coordination of fiber-optic links, more grounded satellite associations, and quicker broadband which has led to a blast as well as the quantity of individuals utilizing the web. On the flip side, this has unintentionally made ready for digital wrongdoing to go after the amazing open doors introduced in East Africa. The growth of cybercrime is detrimental to East Africa's economic and infrastructure development. The transnational element also provides opportunities for organized crime and terror groups to increase their operational capacity. For instance, in Uganda, there has been a massive increase in cyber fraud from 62 cases in 2013 to 198 cases in 2018. In addition to that, in 2020 there was a total of 15b lost through cyber fraud. The bank lost the most while mobile money users who conduct small transactions were also targeted by hackers (Chege, 2021).

There has been an increase in the number of cyber-attacks in Ethiopia according to Ethiopia Monitor, 2021. The Daily News reporter in the country recorded 3,400 reports in the first half of the fiscal year 2021 which was the highest number of recorded crimes in the country. The main areas that were targeted were; infrastructure and websites, accounting for (33%) and (25%) respectively (Shumete Gizaw, 2022). In Tanzania, there were 7000 reports on cybercrimes in 2018, however, this number decreased to 3000 in the year 2020 the numbers were still high (Magalla, 2018).

The African Union (AU) has been working to uphold legislation to combat cybercrime in Africa. The African Union's Convention on Cyber Security and Personal Data Protection 2014 has been endorsed by Rwanda with Uganda and Kenya slowly embracing it. In addition, there have been acts that have come up in Eastern Africa to prevent cybercrimes such as the 2011 Computer Misuse Act (Uganda), Cybercrimes and Computer Misuse Provisional Order 2021(S. Sudan), Cybercrimes Act 2015(Tanzania), Computer Misuse and Cybercrimes Act 2018(Kenya).

1.1.3. Kenyan Perspective

Cyber security in Kenya is governed by various provisions of law including Article 31 of the Constitution of Kenya 2010, The Kenya Information and Communication Act No.2 of 1998, the Computer Misuse and Cyber Crimes Act No. 5 of 2018, and the Data Protection Act No. 24 of 2019. The Kenya Information and Communications Act provides that cyber security refers to

means of collecting the tools, policies, security concepts, guidelines, security safeguards, risk management approaches, actions, best practices, assurance, and technologies that can be used to protect the cyber technologies. The Computer Misuse and Cybercrimes Act does not describe what cyber security entails however it lists some of the cybercrimes. These include cybersquatting, cyber espionage, and phishing, however, the most prominent cybercrimes in Kenya now are false publications where false news is publicized, computer fraud, computer hacking, money transfer fraud, credit card fraud, and cyber terrorism, and computer harassment.

Cybercrime in Kenya has greatly increased over the recent years and has become a growing problem affecting the security of the country. While the greater part of the assaults is designated at large corporations - a larger part with the monetary muscle to support ransoms - medium-sized organizations are not excluded all things considered. The danger has become ten times for organizations during the pandemic as culprits strike-through hacking, phishing, and Ransomware assaults. Kenya which is known as Silicon Savannah is home to a sh120 billion tech hub and over 230 digital service provider start-up businesses. With this hearty data innovation framework set up, Kenya remains an appealing business sector for cybercriminals.

According to business consulting firm Serianu in 2018, Kenya lost about Sh33.5 billion to cybercriminals every year, an amount that has been increasing steadily (Serianu, 2018). According to the communications authority of Kenya (CA), there were 38.8 million cyber threats in three months to June 2021, a 37.3% jump from the 28.2 million cyber-criminal activities identified in the first three months of the same year. In 2020, the number of cybercrimes reported was nearly 140 million, with the most common one being malware which had 124 million reports. National Kenya Computer Incident Response Team (National KE-CIRT) is likewise answerable for the public coordination of network protection as well as Kenya's public resource on digital protection matters. They received a total of 529 reports compared to 298 requests in the previous period.

1.2. Problem statement

The assessment of Information Communication Technology (ICT) crimes and offences in Kenya is a critical undertaking due to the escalating prevalence and severity of cybercrimes in the country. With the rapid advancement of technology and the increasing reliance on digital

platforms for various activities, Kenya has become a fertile ground for cybercriminals, posing significant threats to individuals, businesses, and the nation's overall security and economy.

Despite the existence of laws such as the Computer Misuse and Cybercrimes Act of 2018, the Data Protection Act of 2019, and other relevant provisions, the effectiveness of these measures in curbing ICT crimes remains uncertain. The continuous rise in cyber threats, attacks, and financial losses raises questions about the adequacy of existing cybersecurity frameworks and whether they are capable of keeping pace with the evolving tactics of cybercriminals.

Furthermore, the successful prosecution of cyber culprits remains a challenge, and the lack of local judicial precedents and case law on ICT crimes hinders a comprehensive understanding of the legal landscape. This gap in knowledge limits the development of effective strategies for preventing and combating cybercrimes. Moreover, while various reports and statistics indicate the magnitude of cybercrime in Kenya, there is a notable dearth of comprehensive research on the specific trends, patterns, and motivations driving these criminal activities. An in-depth assessment of the various types of cybercrimes prevalent in the country, their targets, and the methods employed by perpetrators is essential to formulate evidence-based policies and enhance cybersecurity practices.

The challenge of ICT crimes and offences in Kenya is further complicated by the ever-evolving nature of cyber threats, which necessitates continuous monitoring and adaptation of preventive measures. The growing digital transformation across various sectors of society, including government, banking, and businesses, demands a robust cybersecurity framework that can safeguard sensitive data, protect privacy, and maintain the trust of citizens and consumers.

Hence, in light of the increasing complexity and frequency of cybercrimes in Kenya, there is an urgent need for a comprehensive assessment that can identify the loopholes in existing cybersecurity measures, propose effective solutions, and inform policymakers, law enforcement agencies, and relevant stakeholders on the best practices to combat and prevent ICT crimes. Such an assessment will contribute to the development of a resilient and proactive cybersecurity strategy that can safeguard Kenya's digital landscape and ensure the safety and prosperity of its citizens and institutions.

1.3. General objective

The overarching aim of this study is to conduct a study on Information, Communication, and Technology-related (ICT) crimes and offences throughout the country.

1.3.1. Specific objectives

The specific objectives of the study are to:

1. Establish the prevalence of ICT crimes and offences in Kenya.
2. Identify the victims and perpetrators of ICT crimes and offences in Kenya.
3. Ascertain the factors contributing to ICT crimes and offences in Kenya.
4. Determine the effects of ICT crimes and offences in Kenya
5. Ascertain the existing control measures in addressing ICT crimes and offences in Kenya
6. Identify challenges in addressing ICT crimes and offences in Kenya.

1.4. Justification of the study

This study is well-justified for several reasons. Firstly, crimes, including ICT crimes and Offences, pose significant threats to internal security, potentially disrupting peace, and stability, and hindering a country's socioeconomic and political integration. Despite the Kenyan government's substantial allocation of resources towards crime prevention, the increasing number of reported ICT crimes persists, mainly due to the anonymity provided by cyberspace.

While Kenya has implemented various legal, policy, and administrative frameworks to combat cybercrimes, the existing efforts have not effectively addressed the issue. Frameworks such as the National ICT Policy, National Cybersecurity Strategy 2014, and Computer Misuse and Cyber Crimes Act, 2018, exist, but their implementation needs to be enhanced. The study aims to provide empirical evidence to inform effective mechanisms for preventing and combating ICT crimes and Offences.

Another justification lies in the scarcity of comprehensive studies on ICT crimes and offences in Kenya. The lack of reliable and disaggregated data on these crimes has been a challenge. This study seeks to address this gap by conducting an in-depth analysis of patterns, trends, and successes in current interventions. By doing so, it will contribute to a better understanding of the dynamics surrounding ICT crimes and offences in the country.

In summary, this study is justified due to the pressing need to enhance internal security, address the growing threat of ICT crimes, and leverage empirical evidence to improve the implementation of legal, policy, and administrative frameworks. By shedding light on the trends and successes in current interventions, the research will contribute valuable insights towards developing more effective strategies for preventing and combating ICT crimes and offences in Kenya.

1.5. Assumptions of the study

Assumptions in this study refer to the underlying beliefs or premises upon which the research was based. They were not proven facts but were taken as reasonable and necessary for the study to be conducted effectively. Some potential assumptions for this study on ICT crimes and offences in Kenya included:

Data Accuracy and Availability: The study assumes that the data on ICT crimes and offences available from various sources, such as law enforcement agencies and relevant government departments, are accurate, reliable, and comprehensive.

Government's Efforts: The study assumes that the Kenyan government is genuinely committed to addressing ICT crimes and Offences, as evidenced by the allocation of resources and the implementation of legal, policy, and administrative frameworks.

Respondents' Willingness to Participate: The study assumes that individuals and organizations involved in cybercrime incidents will be willing to participate in data collection activities, such as interviews or surveys.

Implementation of Frameworks: The study assumes that the legal, policy, and administrative frameworks in place to combat cybercrimes have been fully implemented and effectively enforced. It also assumes that the existing frameworks are appropriately coordinated and integrated to address the complex and evolving nature of cyber threats.

Generalizability of Findings: The study assumes that the findings and conclusions drawn from the research will have broader applicability beyond the specific sample and context of Kenya.

Level of Awareness: The study assumes that individuals and organizations in Kenya have a reasonable level of awareness and understanding of cyber threats, cybersecurity measures, and the importance of reporting cybercrime incidents.

Effective Interventions: The study assumes that the existing interventions and strategies to combat ICT crimes and offences have the potential to yield positive results. It further assumes

that the study can identify areas of success and areas that require improvement in the current interventions.

These assumptions were carefully considered and validated throughout the research process to ensure the credibility and reliability of the study's findings and conclusions.

1.6. Scope and limitations of the study

The scope of this study was on the analysis of the prevalence, victims, and perpetrators to establish the contributing factors, effects, and impact of ICT-related crimes and Offences, focusing on various sectors and demographics. Additionally, the study investigated the challenges faced by regulatory agencies in handling cybercrime cases recommended interventions, and assessed the level of cyber security awareness among individuals and businesses.

The study was undertaken in 25 counties within the Republic of Kenya with a focus on regulatory agencies and service providers.

1.6.1. Limitations of the study

Time Constraints: Conducting an in-depth study on cybercrimes requires substantial time and resources. Given the time constraints, the study was not able to delve into all aspects of cybercrime in Kenya. Given time constraints, the study prioritized key areas of cybercrimes and offences that have the most significant impact on individuals, businesses, and national security.

Sample Size: The study's sample size may be limited due to practical constraints, potentially impacting the generalizability of findings to the entire population. Researchers made an effort to ensure a diverse and representative sample to enhance the generalizability of the study's findings.

Technological Advancements: Rapid changes in technology and cyber threats may render some of the study's findings less relevant over time.

1.7. Theoretical framework

In this study, three criminology theories that are; Routine Activity Theory, Rational Choice Theory, and Social Learning Theory were considered to provide a theoretical framework for understanding cybercriminal behavior, motivations, and the effectiveness of crime prevention strategies. Their proponents, basic tenets, strengths, and their relationships to the study's objectives were factored in:

Routine Activity Theory: The theory was pioneered by Lawrence E. Cohen and Marcus Felson (1979). The basic tenets of Routine Activity Theory posit that for a crime to occur, three elements must converge in time and space: a motivated offender, a suitable target, and the absence of capable guardianship. It focuses on the daily routines and activities of individuals and how they create opportunities for criminal acts. Strengths: Routine Activity Theory applies to various types of crimes, including cybercrimes, and provides insights into the factors that increase vulnerability to Offences. It can help identify areas where cybercrime prevention efforts need strengthening and where capable guardianship (e.g., effective cybersecurity measures) can be enhanced. The relationship to the Study's Objectives is that it can help explain the patterns and trends of ICT crimes in Kenya. By identifying high-risk situations and weak points in cyber security, the study can inform targeted crime prevention strategies to reduce opportunities for cybercriminals.

Rational Choice Theory: The theory was pioneered by Ronald V. Clarke (1983) The, basic tenets of Rational Choice Theory suggest that individuals make rational decisions based on a cost-benefit analysis of potential risks and rewards. In the context of cybercrimes, offenders weigh the benefits of illicit gains against the perceived risks of being caught and punished. Strengths: Rational Choice Theory provides insights into the decision-making processes of cyber criminals and the incentives driving their actions. Understanding the rationality behind cybercriminal behavior can inform strategies to increase the perceived risks and reduce the attractiveness of engaging in cybercrimes. The relationship to the Study's Objectives is that the study can explore the motivations of cyber criminals in Kenya and assess the effectiveness of current crime prevention efforts in deterring potential offenders.

Social Learning Theory: The theory was pioneered by Albert Bandura (1977). The basic tenets of Social Learning Theory posit that people learn behavior by observing others and the consequences of their actions. In the context of cybercrimes, individuals may be influenced by peers, media, or online communities promoting or normalizing illicit activities. Strengths: Social Learning Theory helps to understand the role of social influences and peer groups in shaping cybercriminal behavior. It can shed light on the social mechanisms that foster cybercrime and inform interventions to counter these influences. The relationship to the Study's Objectives is that the study can explore the social dynamics surrounding ICT crimes in Kenya, identify

potential sources of influence on cybercriminals, and recommend awareness and prevention programs targeting specific social groups or online communities.

Integrating these relevant theories into the study can provide a solid theoretical foundation for understanding the dynamics of ICT crimes and offences in Kenya. By examining cybercriminal motivations, risk perception, and social influences, the research can offer valuable insights into the factors driving cybercrimes and inform evidence-based crime prevention strategies and policies.

CHAPTER TWO: METHODOLOGY

2.1. Introduction

This chapter presents the research design, study population, unit of analysis, sample size and sampling procedures, data collection and management methods, data analysis techniques, and ethical considerations employed in the study on Information Communication Technology (ICT) crimes and offences in Kenya.

2.2. Research design

The study utilized a descriptive research design to provide a comprehensive description of the characteristics of ICT crimes and offences in Kenya. This design facilitated extensive data gathering and enabled the estimation of proportions and predictions related to cybercrime trends.

2.3. Study population and unit of analysis

Table 1: Institutions sampled in the study

Institution of affiliation	**National Police Service/DCI**
	Money Transfer agents (Mpesa by Safaricom, Airtel Money)
	Digital service vendors
	Financial Institutions (Banks, Saccos, Insurance Companies,
	Kenya Prisons Service
	Probation and Aftercare Service
	National Government Administrative Offices (NGAO)
	Mobile network providers (Airtel, Safaricom, Telkom (Any other)
	Judiciary (Law Courts)
	Office of the Director of Public Prosecutions
	Department of Children Services
	Information and Communication Technology (ICTA)
	Ministry of ICT, and the Digital Economy
	Communication Authority of Kenya (CA)
	National Computer and Cybercrimes Coordination Committee (NC4)
	Office of Data Protection Commissioner (ODPC)
	The state department of social protection and senior citizen affairs
	National Intelligence Service
	Ministry of Youth and Sports
	County Government
	Ministry of labour and social protection
	Kenya Revenue Authority

The study population consisted of service providers and regulatory agencies from all 47 counties in Kenya. The study sampled regulatory agencies associated with the Criminal Justice System (National Police Service, Office of the Director of Public Prosecutions, Directorate of Children Services, Judiciary, Kenya Prisons Services, and Probation and Aftercare Services) other regulatory agencies in the ICT sectors: NC4, Ministry of Information, Communication, and Digital Economy, ICTA among others) were interviewed. Furthermore, stakeholders from both state and non-state entities within the ICT sector deemed knowledgeable about the subject matter due to their work within the sector, were also included in the study. The respondents were drawn from various institutions in 25 sampled counties in Kenya as in Table 1.

2.3.1. Sample size and Sampling procedure

The study employed a combination of stratified and purposive random sampling techniques. The stratified random sampling aided in capturing key population features within the primary target population and enhanced precision while minimizing errors. The strata consisted of regulators and service providers in the ICT sector, enabling tracking and monitoring of key indicators related to crime and security threats. Key informants were purposively selected from other relevant government institutions, considering their knowledge of the work operations. The study targeted 25 counties out of the 47 counties in Kenya and then purposively targeted 2 sub-counties within the county, the targeted sub-counties were within an urban setup due to the nature of the study. The study targeted a total of 2254 respondents for the interviews and achieved a sample size of 2100 representing a response rate of 93.1%.

2.4. Methods and Tools of data collection

2.4.1. Data collection methods

The study gathered both primary and secondary data. Primary data was collected through face-to-face interviews and discussions with sampled respondents. Secondary data was obtained by reviewing existing reports and relevant publications from credible sources to complement the primary data.

2.4.2. Data Collection Tools

Data was collected using questionnaires with both closed and open-ended questions. Quantitative data from sampled respondents (service providers and regulatory agencies) was collected

through face-to-face interviews using a structured questionnaire. Secondary data was gathered by mining, analyzing, and collating information from secondary sources.

2.4.3. Data Collection and Management Procedure

The interview schedule and questionnaire were prepared and pre-tested in a sub-county not included in the target population. The pre-test was to assess the reliability and validity of the questions for successful data acquisition. Competent research assistants were trained before the actual data collection.

2.5. Data processing and analysis

Quantitative data was analyzed using Statistical Package for Social Sciences (IBM SPSS) version 24 analysis software and presented using frequencies, percentages, tables, charts, and figures to provide a clear picture of the findings.

2.6. Ethical consideration

The study obtained informed consent from all participants by providing them with a clear explanation of the research purpose, duration, and potential use of the findings. Participants were informed of their rights to withdraw from the study if they wished. Confidentiality and anonymity were ensured, and no information was used to jeopardize the welfare of the participants. Ethical guidelines were followed, and the participants will be given access to the final research outcome.

CHAPTER THREE: FINDINGS AND DISCUSSIONS

3.1. Introduction

This chapter presents the research findings and their implications. It also provides the social demographic profile of the respondents and thematic areas of the study.

3.2. Social demographic characteristics of the respondents

Gender Distribution: The data shows that there is a higher representation of male respondents (58.3%) compared to female respondents 41.7%. This could imply that men are more willing to participate in the study or are more accessible for data collection. However, it might also indicate a potential gender bias in the study, as the experiences and perspectives of women regarding ICT crimes and offences may not be adequately represented.

Age Representation: Most respondents fall within the age group of 18-34 years (55.1%). This suggests that the study is predominantly capturing insights from younger individuals who are more tech-savvy and likely to be active in the digital space. The age distribution of respondents may impact the study's understanding of ICT crimes and Offences, particularly about how different age groups are affected by cybercrimes. Older age groups may have different vulnerabilities and risk perceptions, which could be underrepresented in the study.

Educational Background: A significant proportion of respondents (43.7%) have attained a university education. This indicates a relatively educated sample, which may have a higher awareness of cyber risks and preventive measures. The high level of education in the sample could influence the study's findings, as educated individuals may have a better understanding of cyber threats and adopt safer online practices.

Main Occupations: The study respondents came from diverse occupational backgrounds, with the highest representation being from the public sector at (49.2%) and businesspersons at 25.2%.The occupational diversity in the sample could influence the study's findings, as individuals from different professions may encounter distinct types of ICT crimes and Offences.

Table 2: Demographic Characteristics of the Respondents

Characteristics	Categories	Percentage
Main occupation	permanent employment- private sector	10.7%
	permanent employment - public sector	49.2%
	casual, temporary employment	14.8%
	business person	25.2%
The highest level of education attained	Primary	0.7%
	Secondary	23.1%
	Middle-level college	32.2%
	University	43.7%
	adult literacy	0.1%
Gender	Male	58.3%
	Female	41.7%
Age	18-34	55.1%
	35-51	39.0%
	52-68	5.8%
	69+	0.1%

Source: Field data

3.3. Prevalence of ICT crimes and offences

Overall, the data indicates that a significant number of respondents believe that ICT crimes and offences are a serious issue in Kenya, which highlights the importance of addressing this problem through effective prevention and mitigation strategies. The majority of respondents (67.5%) rated the prevalence of ICT crimes and offences as high, indicating that these crimes are widespread and significant in Kenya.

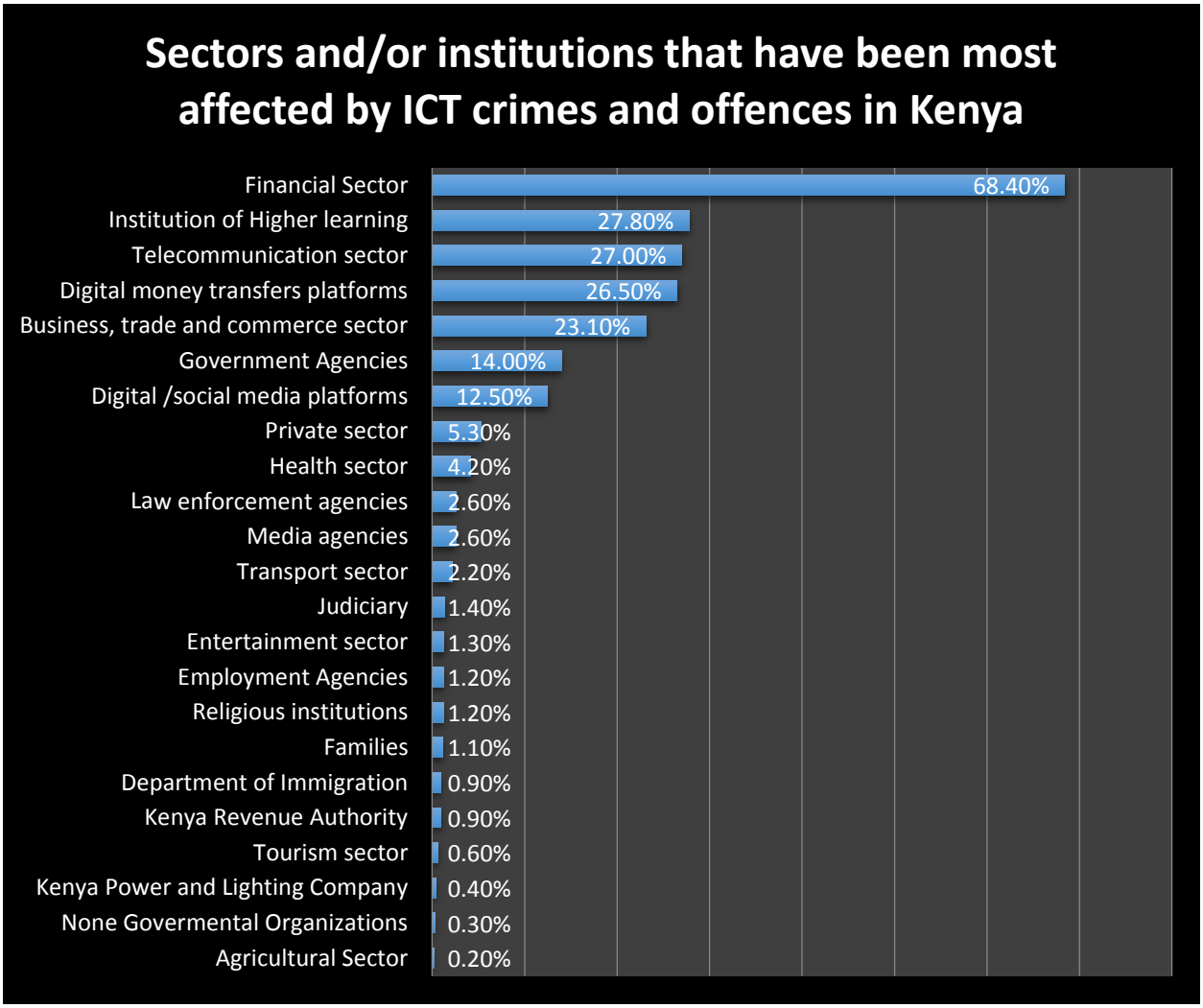
A considerable proportion of respondents (29.3%) also rated the prevalence as a medium, suggesting that ICT crimes and offences are moderately prevalent in the country. Only a small percentage of respondents (3.3%) considered the prevalence to be low, implying that some respondents perceive ICT crimes and offences to be less common.

3.3.1. Sectors and/or institutions affected by ICT crimes and offences in Kenya

From the data analysis, it's evident that the reach of Information and Communications Technology (ICT) crimes and cyber offences spans across a diverse range of sectors in Kenya. The most impacted sector by far is the Financial Sector, where a staggering (68.4%) of reported cases involve offences such as online banking fraud, credit card scams, and phishing attacks that specifically target financial institutions. This underlines the urgent need for stringent cyber security measures within the financial ecosystem to protect both the institutions and their clients.

The Education and Higher Learning Sector also faces a significant threat, with (27.8%) of reported cases being linked to cyber threats against educational establishments like universities, colleges, and online learning platforms. This underscores the importance of safeguarding academic data and intellectual property. Not far behind is the Telecommunication Sector, accounting for (27.0%) of reported cases. These incidents affect not only the telecommunication companies themselves but also their broad customer base, making network security a critical concern.

Interestingly, Digital Money Transfers are also susceptible to cyber threats, making up (26.5%) of reported cases. Popular platforms like MPesa and Airtel Money appear to be targets for cybercriminals, emphasizing the need for stronger verification processes and user education. The Business, Trade, and Commerce sectors follow closely, constituting (23.1%) of cases. Cybercrimes in this sector can have a detrimental effect on the Kenyan economy, affecting everything from small businesses to large trade operations. Government agencies are not immune either; (14.0%) of reported cases involved cyber threats aimed at various governmental bodies. This could have widespread implications for public services and national security. Additionally, the rise of the digital age brings with it new forms of vulnerabilities. Digital and Social Media Platforms account for (12.5%) of the reported cases. These platforms are increasingly becoming grounds for misinformation, privacy violations, and other forms of cyber exploitation.



Source: Field data

Figure 1: Sectors and/or institutions affected by ICT crimes and offences in Kenya

Meanwhile, the Private Sector and Health Sector represent 5.3% and 4.2% of reported cases, respectively. Even though these figures are relatively lower, the sensitivity of health data and corporate secrets means that any cyber-attack can have disproportionately severe consequences. Media Institutions face their own set of challenges, making up 2.6% of reported cases. These threats could potentially compromise journalistic integrity and freedom, impacting the democratic fabric of society.

3.3.2. Prevalence of ICT crimes and offences in Kenya

In Kenya, the landscape of Information and Communications Technology (ICT) crimes and cyber offences is both wide-ranging and worrisome. Topping the list is Computer Fraud, which accounts for an alarming (72.9%) of reported cases. Such fraud often exploits weaknesses in computer systems to deceive individuals or organizations for financial benefits. This glaring statistic stresses the need for advanced cybersecurity measures, routine system audits, and comprehensive employee training to fend off fraudulent activities.

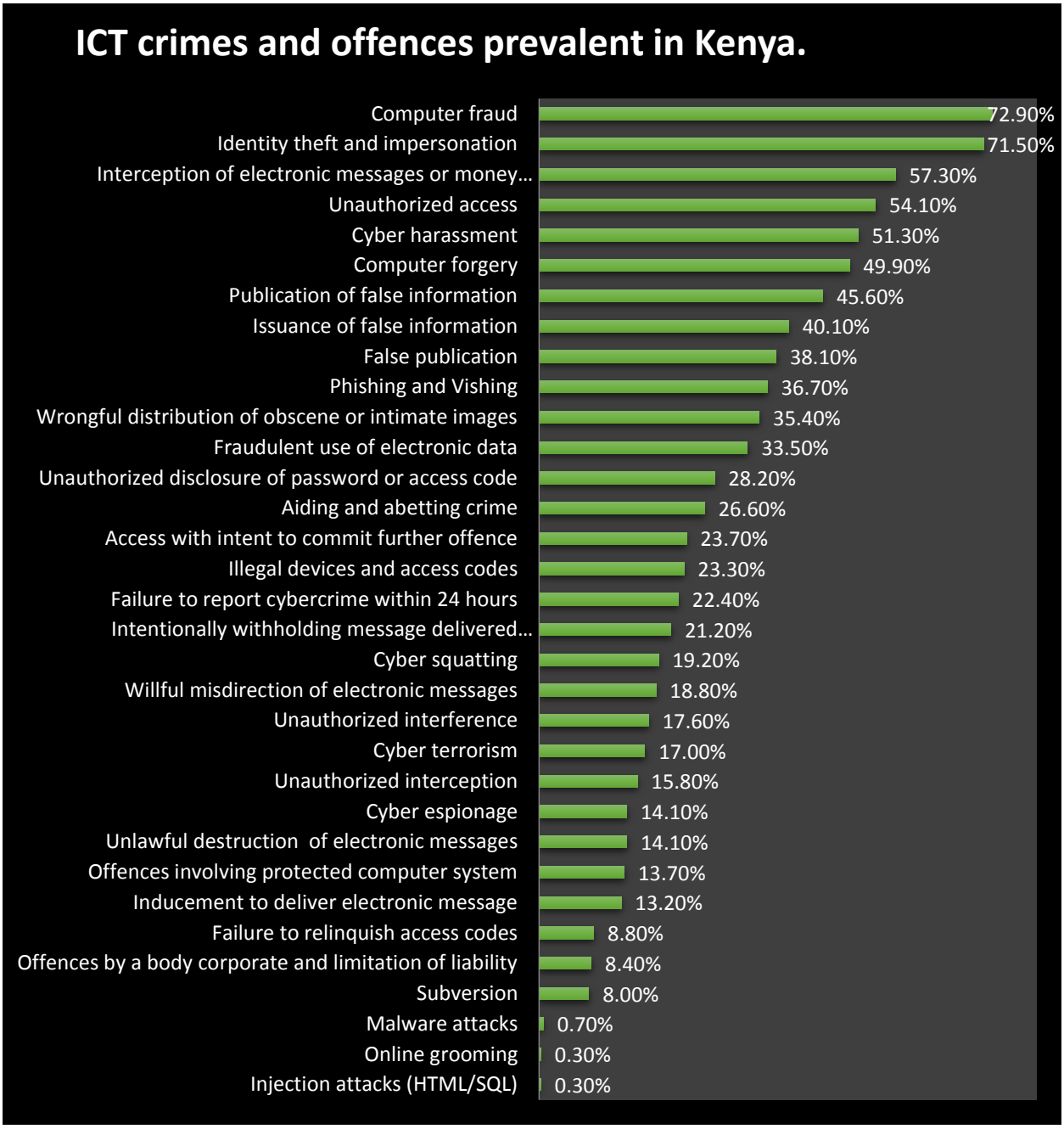
Following closely is Identity Theft and Impersonation at (71.5%). This nefarious practice involves stealing personal data to impersonate individuals for illicit purposes, from financial gain to defamation. The alarming prevalence suggests an urgent need for robust authentication and encryption techniques to secure sensitive information against unauthorized access.

Interception of Electronic Messages or Money Transfers is another significant issue, constituting (57.3%) of reported cases. This fact emphasizes the vulnerabilities in communication channels and financial transactions. It suggests the critical need for secure communication protocols and fraud detection mechanisms to minimize risks.

Unauthorized Access is also rampant, with (54.1%) of incidents highlighting a breach in computer systems. This necessitates stronger access control measures that might include multi-factor authentication and frequent password updates to keep unauthorized users at bay.

Cyber Harassment is a pervasive issue, affecting (51.3%) of the population. Its prevalence underscores the need for heightened awareness, support structures for victims, and stricter legislation against online harassment and cyberbullying.

Computer Forgery constitutes (49.9%) of reported cases and is a clear sign that cybercriminals are adept at creating or altering electronic documents for deceitful purposes. The introduction of digital signature technologies and document verification methods can help combat this form of cybercrime.



Source: Field data

Figure 2: prevalence of ICT crimes and offences in Kenya

Concerning misinformation, both the Publication of False Information (45.6%) and the Issuance of False Information (40.1%) rank highly. These percentages indicate a dire need for media literacy campaigns and responsible information-sharing practices to curb the spread of falsehoods.

Phishing and Vishing, at (36.7%), remain prevalent cyber threats. These deceptive methods often lure unsuspecting victims into revealing sensitive information, stressing the need for sensitization programs to the public on such scams.

Wrongful Distribution of Obscene or Intimate Images accounts for (35.4%) of cases, violating privacy and causing emotional distress.

Fraudulent Use of Electronic Data, constituting (33.5%) of reported cases, can wreak financial havoc for individuals and organizations alike. Strong data protection measures and stringent monitoring of data access can go a long way in mitigating this threat.

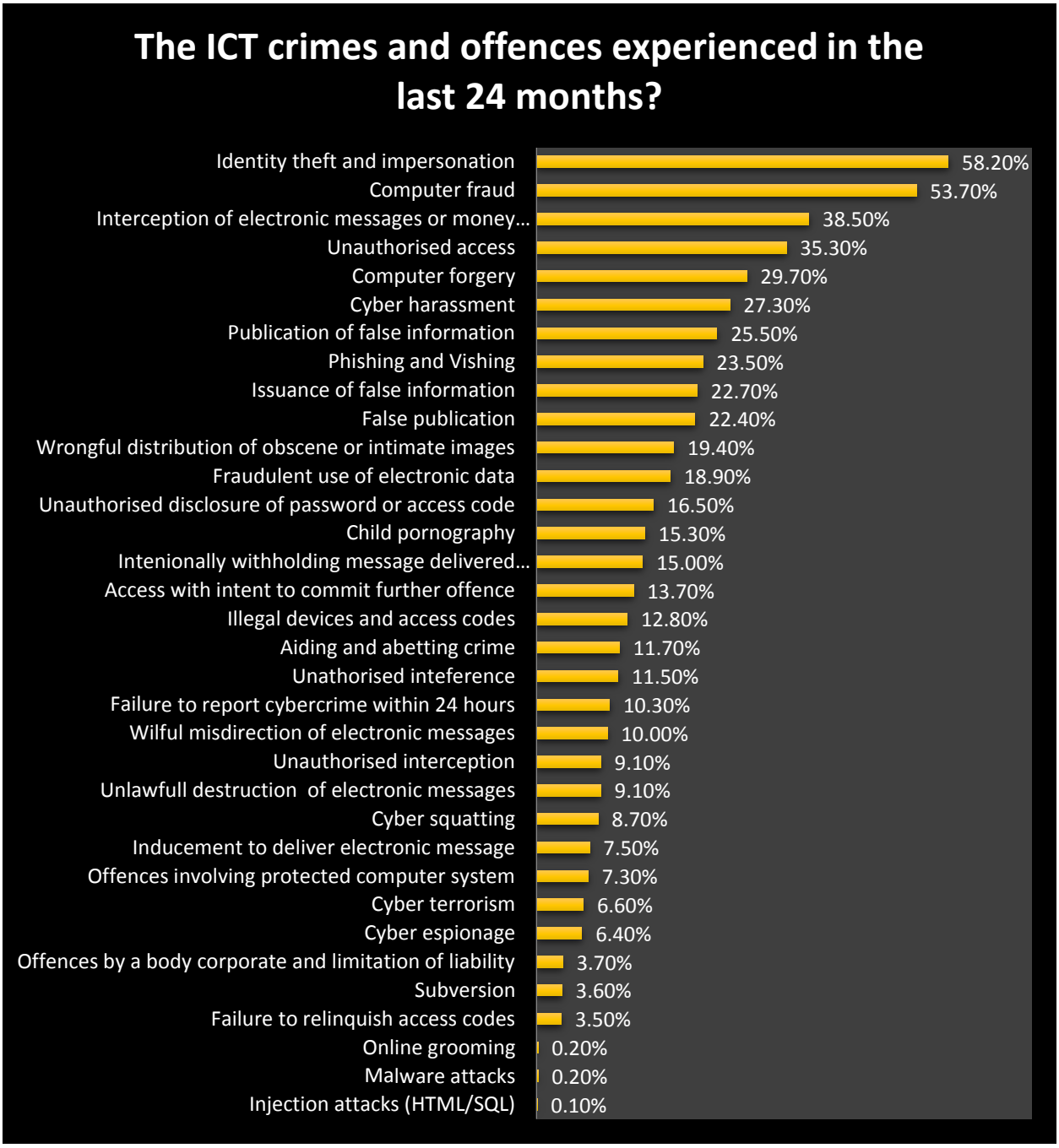
Finally, Unauthorized Disclosure of Password or Access Code comprised (28.2%) of reported cases, compromising individual and organizational cybersecurity. This calls for the need to sensitize users about secure password practices and implement strict access control policies to prevent unauthorized access or disclosure.

From the foregoing, the array of cyber threats plaguing Kenya is extensive, necessitating a multi-faceted approach that combines technological solutions, legislative action, and public awareness campaigns to better secure the digital landscape.

3.3.3. Experiences of ICT crimes and offences in the last 24 months

From the study findings, the majority (84.8%) of respondents reported experiencing some form of ICT crimes and offences in the last 24 months, while only (15.2%) stated that they had not encountered any such incidents during that period.

From the Information and Communications Technology (ICT) crimes in this study, Identity Theft and Impersonation top the list as the most prevalent, with (58.2%) of respondents acknowledging encounters with this form of cybercrime. The statistics suggest a pressing need for enhanced identity protection measures to safeguard personal information from unauthorized access and fraudulent use.



Source: Field data

Figure 3: The ICT crimes and offences experienced in the past 24 months

Notably, Computer Fraud was cited by (53.7%) of respondents as the second most common form of cybercrime they've encountered. This percentage emphasizes the critical nature of safeguarding financial transactions and sensitive data from manipulation and deception.

Interception of Electronic Messages or Money Transfers is another worrisome trend, reported by (38.5%) of respondents. This finding calls for the need for secure communication channels and fortified online banking systems to prevent unauthorized interventions in both personal and professional exchanges.

Cyber Harassment, affecting (27.3%) of respondents, is a significant issue that poses a risk to individual well-being and mental health. The prevalence of this form of abuse underscores the importance of implementing measures to protect online users from harassment and bullying.

Phishing and Vishing attacks have been experienced by (23.5%) of respondents, emphasizing the essential role of cybersecurity awareness and education. Individuals must be trained to recognize and fend off these manipulative attempts to extract sensitive information.

Alarmingly, Child Pornography is reported by (15.3%) of respondents, drawing attention to the urgency of implementing stringent measures to eradicate this horrific crime and ensure the safety of children in online spaces.

While less frequent in occurrence, both Cyber Terrorism and Cyber Espionage are nevertheless critical concerns, affecting (6.6%) and (6.4%) of respondents respectively. Despite their relative rarity, these threats to national security require immediate and robust countermeasures at the government level to mitigate risks.

Lastly, even though Malware Attacks and Injection Attacks are exceedingly rare, affecting just (0.2%) and (0.1%) of respondents respectively, their presence should not be overlooked. These forms of cybercrime indicate the need for comprehensive cybersecurity solutions to detect and neutralize threats before they can harm.

In summary, the prevalence and variety of cyber threats underscore a compelling need for a multi-faceted strategy encompassing robust cybersecurity measures, public awareness campaigns, and stringent legal repercussions for perpetrators.

3.4. Victims and perpetrators of ICT crimes and offences

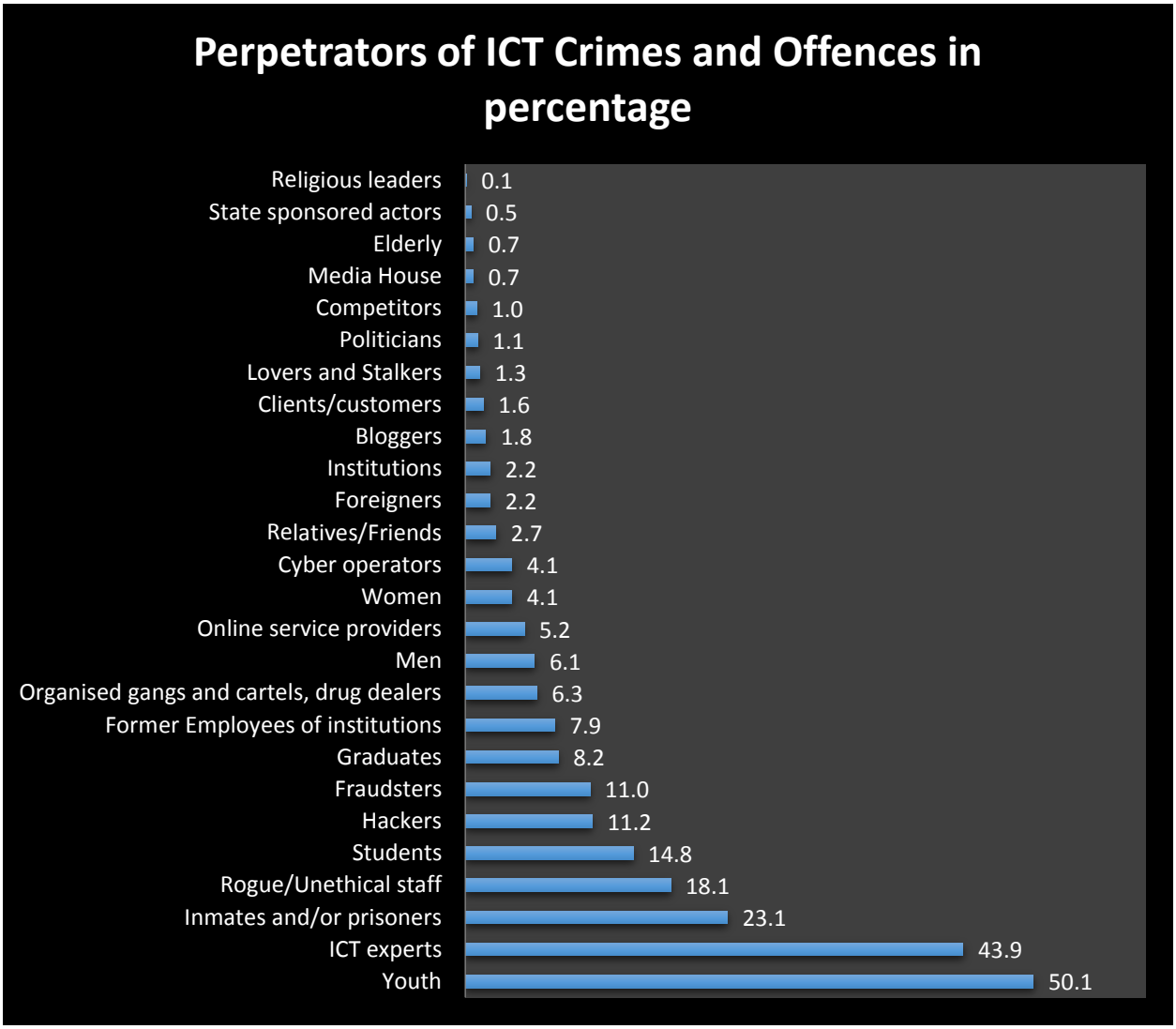
3.4.1. Perpetrators of ICT crimes and Offences

The study highlights the most prominent category of perpetrators, as mentioned by more than (10%) of the respondents. The percentages represent the proportion of respondents who identified each category as being involved in committing ICT crimes and Offences. The most prominent category was youths, (50.1%) of respondents believe that young individuals, typically in the youth age group, are involved in ICT crimes and offences.

The second category was ICT experts, (43.9%) of respondents suspect that ICT experts, professionals with advanced knowledge of information and communication technology, are engaged in perpetrating cybercrimes. The third category was the inmates and/or prisoners, (23.1%) of respondents mentioned inmates and/or prisoners as potential perpetrators of ICT crimes and Offences.

The fourth category of perpetrators was rogue/unethical staff, (18.1%) of respondents pointed out that rogue or unethical staff within organizations might be involved in cybercrimes. The fifth category was students, (14.8%) of respondents believe that students, particularly those with technical skills, could be involved in committing ICT crimes and Offences. The sixth category was hackers, (11.2%) of respondents identified hackers, individuals with advanced computer skills who exploit system vulnerabilities, as possible perpetrators. The seventh category mentioned by the respondents was fraudsters, (11.0%) of respondents suspect that fraudsters, individuals who engage in fraudulent activities, are involved in ICT crimes and Offences. The figure below illustrates the findings of the study.

This study aimed to uncover the individuals responsible for crimes within the ICT sector. According to the responses received, a predominant group of perpetrators pointed out by the respondents were youths, accounting for (50.1%) of the cases, and ICT experts (43.9%). The study also delved into prevalent cybercrimes and identified five major types that frequently occur. These types included identity theft and impersonation, computer fraud, interception of electronic messages or money transfers, unauthorized access, and computer forgery.



Source: Field data

Figure 4: Perpetrators of ICT crimes and offences in Kenya

These crimes inherently demand a certain level of technological proficiency for successful execution, thus the mention of youths as the primary perpetrators is not merely coincidental. The motivations driving these cybercrimes vary widely. On one end of the spectrum, individuals are aiming for personal financial gain through activities like online fraud, identity theft, and phishing attempts. On the other end, there exist more sophisticated groups involved in intricate acts such as data breaches, ransomware attacks, and various forms of cyber extortion.

In recent years, the country has witnessed a surge in educated yet unemployed youths. Elevated levels of youth unemployment can result in frustration, disillusionment, and social unrest. Unemployed youths, particularly when facing limited opportunities, might become more susceptible to involvement in criminal acts, protests, and even extremism as a means to express their frustrations. The significant percentage of

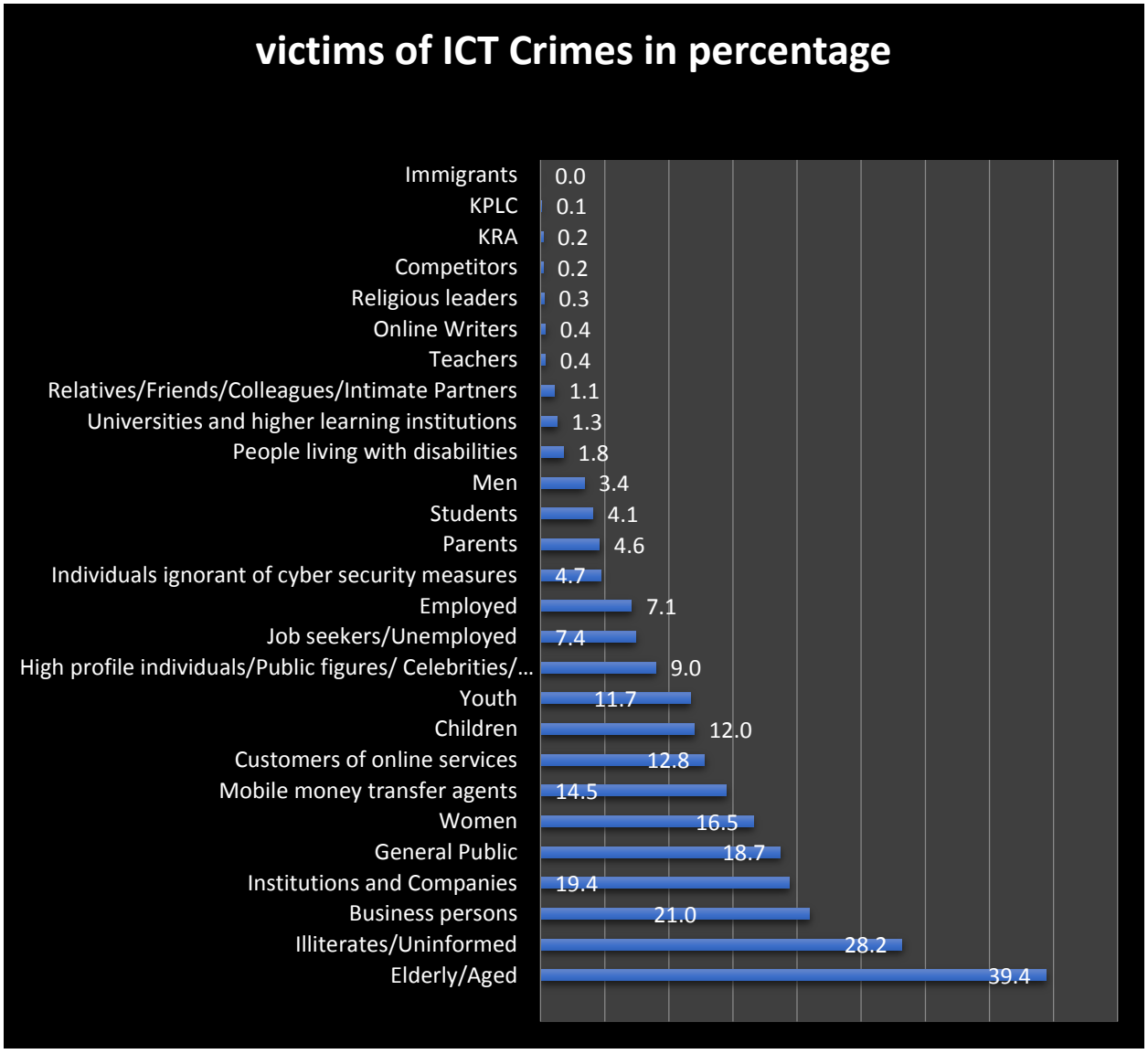
youth involved in ICT crimes indicates a need for focused interventions to address the factors that lead young individuals towards cybercriminal activities, such as education and awareness programs. These awareness and cyber security educations should target youth, students, and ICT experts to promote ethical use of technology and deter involvement in cybercrimes.

The presence of rogue/unethical staff and former employees as potential perpetrators highlights the importance of robust internal security measures within organizations to prevent data breaches and misuse of information. To mitigate insider threats organizations should implement strict access controls, regular security audits, and employee training to prevent rogue/unethical staff and former employees from exploiting vulnerabilities. The involvement of ICT experts and graduates in cybercrimes underscores the necessity of fostering a strong ethical cyber security culture and promoting responsible use of technical skills. The identification of specific groups like hackers and fraudsters as potential perpetrators indicates the need for specialized training and expertise within law enforcement agencies to effectively combat cybercrimes.

3.4.2. Victims of ICT crimes and offences in Kenya

According to the data, the main victims of ICT crimes and offences in Kenya are as follows: Elderly/Aged, (39.4%) of the respondents identified the elderly or aged population as the main victims of ICT crimes, highlighting their vulnerability to cyber exploitation. Illiterates/Uninformed: (28.2%)of Illiterates/Uninformed, (28.2%) of respondents reported illiterate or uninformed individuals as victims, indicating that lack of knowledge about cyber security exposes them to cyber threats. Business persons, (21.0%) of respondents mentioned business persons as victims, suggesting that cybercriminals target them for financial gains or to disrupt their operations.

There other categories were institutions and Companies, (19.4%) of respondents reported institutions and companies as victims, indicating that cybercrimes pose risks to their data, operations, and reputation. Another category was the general public, (18.7%) of respondents mentioned the general public as victims, indicating that anyone using digital technology is at risk of becoming a victim of cybercrimes.



Source: Field data

Figure 5: Victims of ICT crimes and offences in Kenya

The data indicates that certain demographics, specifically the elderly, individuals with limited literacy, and people with disabilities, are more prone to falling victim to ICT crimes. This susceptibility arises from their constrained grasp of cyber threats and security protocols. Consequently, there arises a crucial necessity to establish targeted cybersecurity awareness and educational initiatives tailored to these vulnerable groups. This strategic approach aims to equip the elderly, those with limited literacy, and people with disabilities with the requisite knowledge and protective measures to safeguard them. The study's findings identified the techniques employed by perpetrators to carry out ICT crimes. The three main methods encompass phone

calls, hacking, and messages. Remarkably, these methods have the potential to impact anyone with a phone, highlighting their widespread reach and potential impact. Given that the elderly often possess a perception of being less technologically inclined, it is plausible that this perception contributes to their vulnerability, making them primary targets for such crimes.

The victimization of the general public, including students and employed individuals, highlights the importance of promoting cybersecurity awareness and best practices among all user groups. Public cyber security campaigns should be launched to educate the general public, students, and job seekers about cyber security risks, safe online behavior, and methods to protect personal information. Reporting and support mechanisms are also important aspects of dealing with cyber crimes, establishing accessible and confidential reporting mechanisms for cybercrime victims, along with support services to assist them in recovering from the impact of cyber incidents.

It is also worth noting that children (12.8%) are also featured as victims of cyber crimes. The victimization of children underscores the importance of implementing strict measures to protect them from cyberbullying, online harassment, and exposure to harmful content. Online child protection measures include parental controls and educational programs, which can safeguard children from cyber threats.

3.4.3. Modus Operandi of ICT crimes and offences in Kenya

The data shows the various methods or *modus operandi* through which ICT crimes and offences are committed in Kenya. The findings highlight the top-mentioned ways of committing crimes by more than ten percent of the sampled population. They include phone Calls (38.1%); hacking (36.8%); messages(27.6%); impersonation/Identity theft (25.1%); deception/Manipulation (17.7%) and scamming, (10.5%). The least mentioned ways of committing ICT crimes and offences were the sim card registration process (0.8%) and pyramid schemes (0.4%). The findings are illustrated in the table 2.

Table 3: modus operandi of ICT crimes and offences in Kenya

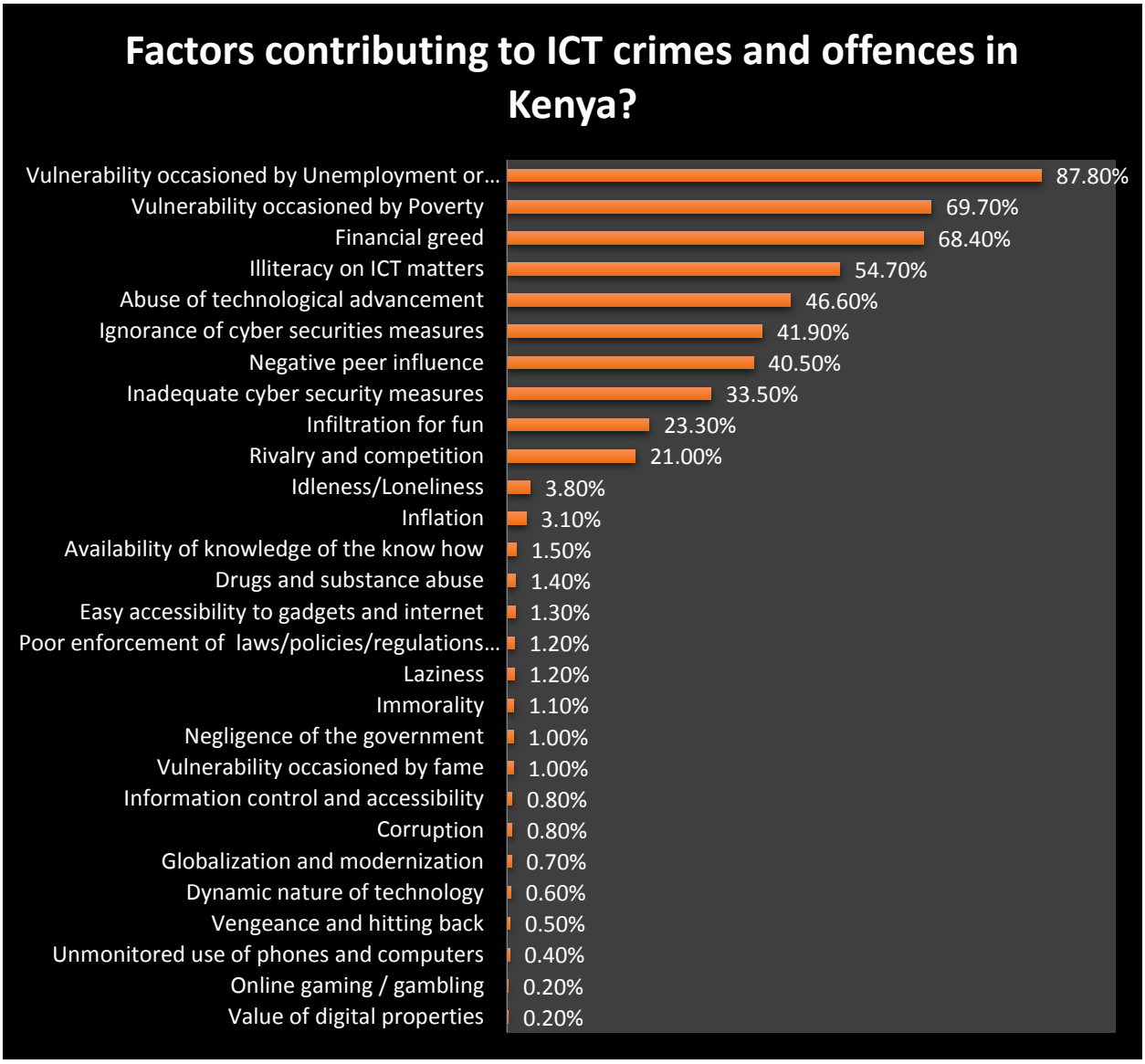
Modus Operandi	Percent of Cases
Phone calls	38.1%
Hacking	36.8%
Messages	27.6%
Impersonation/Identity theft	25.1%
Deception/Manipulation	17.7%
Scamming	10.5%
Through internet	8.9%
Account/Contact cloning	8.3%
Publishing Audio/Videos/Images/Text on social media platforms	7.4%
Spamming	6.9%
Intruder access	6.5%
Access to devices with intent to commit offences	5.9%
Malware/Ransomware	5.6%
Forgery	5.1%
Collusion	3.9%
Blackmail	3.5%
Social engineering	3.2%
Interception of electronic money transfers	2.8%
Using computers to transfer unauthorized info	2.8%
Use of threats	2.7%
Use of special codes	2.6%
Use of pseudo accounts	1.9%
Reversals of transactions	1.6%
SIM card registration process	0.8%
Pyramid schemes	0.4%

Source: Field data

The study implications on the Modus operandi suggest a myriad of measures to address the challenge of cyber security. The high mention of the use of messages (27.6%) of respondents implies that criminals use messaging platforms to carry out their illicit activities. The prevalence of hacking, phishing, and social engineering indicates the need for heightened cyber security awareness among individuals and organizations to protect themselves from such attacks. The use of impersonation and identity theft (25.1%) points out that criminals commit ICT crimes through impersonation or identity theft. This use of fake identities for fraudulent purposes highlights the importance of robust data protection measures to safeguard personal and sensitive information. Scams and deception are common methods used by criminals, and public awareness campaigns are crucial to educate individuals about common cyber threats and how to avoid falling victim to them. The high occurrence of identity theft highlights the importance of implementing identity

theft protection measures to safeguard personal information. The prevalence of ICT crimes carried out through the internet underscores the significance of Internet safety practices for both individuals and organizations

3.5. Factors contributing to ICT crimes and offences



Source: Field data

Figure 6: Factors contributing to ICT crimes and offences in Kenya

According to the data collected, several key factors contribute to the high incidence of Information and Communication Technology (ICT) crimes in Kenya. Among these are economic vulnerabilities such as unemployment and poverty, psychological motives like financial greed,

and societal shortcomings including illiteracy on ICT matters and the misuse of advanced technology.

A staggering (87.8%) of respondents believe that unemployment or underemployment is a significant catalyst for ICT crimes. In a country where job opportunities are scarce, some individuals may turn to cybercriminal activities as a last resort for financial survival. Closely related to this is the issue of poverty, which (69.7%) of respondents identified as a driving force behind cybercrimes. The economic hardships that stem from poverty can push people to seek illicit means to improve their financial standing.

Financial greed was also highlighted by (68.4%) of respondents as a major contributing factor. This suggests that even in the absence of financial desperation, the lure of easy money can lead individuals down a path of criminal activity in the digital space. Another contributing factor is illiteracy in ICT matters, with (54.7%) of respondents noting that a lack of understanding or knowledge about ICT can make individuals susceptible to exploitation and manipulation online. Also, (46.6%) of respondents pointed out that the abuse and misuse of technological advancements contribute to the prevalence of ICT crimes, as criminals exploit these technologies for malicious purposes.

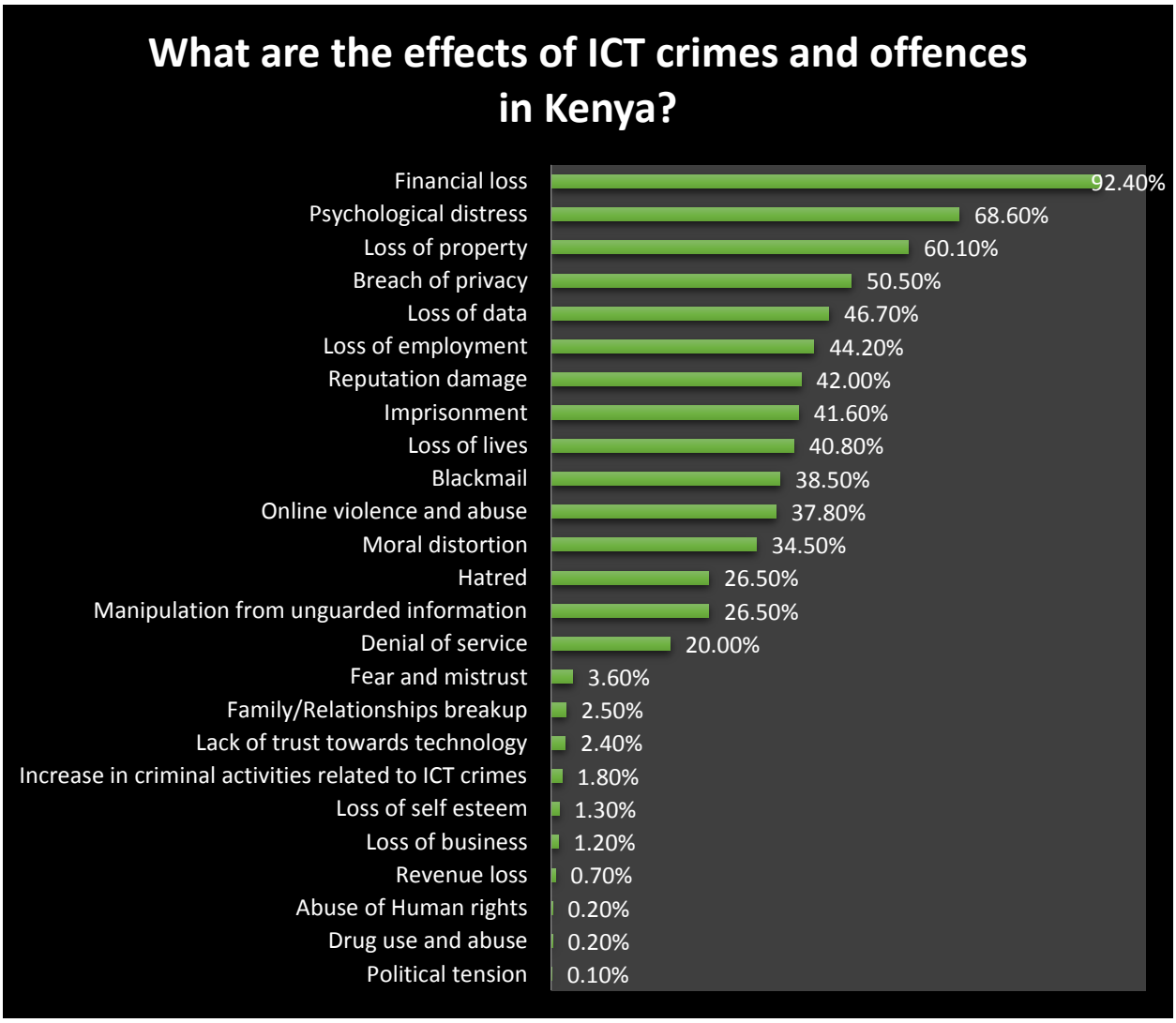
The devastating effects of Information and Communication Technology (ICT) crimes in Kenya reach far beyond the digital realm, permeating various aspects of daily life. According to a recent survey, the consequences are wide-ranging and deeply impactful, affecting both individuals and organizations in profound ways.

The most immediate and quantifiable effect is financial loss, with an overwhelming (92.4%) of respondents reporting monetary setbacks due to cybercrimes. These losses not only deplete individual savings but can also have crippling implications for organizations, disrupting operations and draining resources.

A significant number of respondents, (68.6%), experienced psychological distress as a result of falling victim to cybercrimes. This highlights the emotional and mental health toll that cyber attacks can impose, affecting people's well-being and overall quality of life. The impact of ICT

crimes also extends to the physical world, as (60.1%) of respondents reported a loss of property, indicating that cybercrimes can often lead to tangible damage and theft of valuable assets.

3.6. Effects of ICT crimes and offences



Source: Field data

Figure 7: Effects of ICT crimes and offences in Kenya

In a world where privacy is increasingly scarce, (50.5%) of respondents experienced breaches of their personal and confidential information, potentially leading to a myriad of further complications. Data loss, reported by (46.7%) of respondents, has severe ramifications, especially for businesses and organizations. It can disrupt operations, compromise security, and severely tarnish reputations.

Unemployment as a direct result of cybercrimes was reported by (44.2%) of respondents. This indicates that the repercussions of ICT offences can devastate livelihoods, leaving people without a stable source of income. Further, reputational damage afflicted (42.0%) of respondents, diminishing their standing both personally and professionally.

Legal ramifications, including imprisonment, were cited by (41.6%) of respondents, emphasizing the grave consequences of involvement in ICT crimes. Astonishingly, (40.8%) reported a loss of lives due to cybercrimes, bringing to light the fatal consequences that can arise in certain instances. Blackmail was experienced by (38.5%), indicating the malicious use of sensitive information for illicit gains.

Online violence and abuse were faced by (37.8%) of respondents, which underscores the pervasive negative impact of cyberbullying and harassment in digital spaces. Finally, (34.5%) reported experiencing moral distortion, suggesting that the perpetration or victimhood of cybercrimes can lead to ethical compromises and moral dilemmas.

In sum, the effects of ICT crimes in Kenya are devastatingly comprehensive, affecting financial stability, emotional health, personal reputation, and even life itself. As such, the need for immediate and multi-faceted interventions to combat these crimes is critically urgent.

3.7. Control measures in addressing ICT crimes and offences

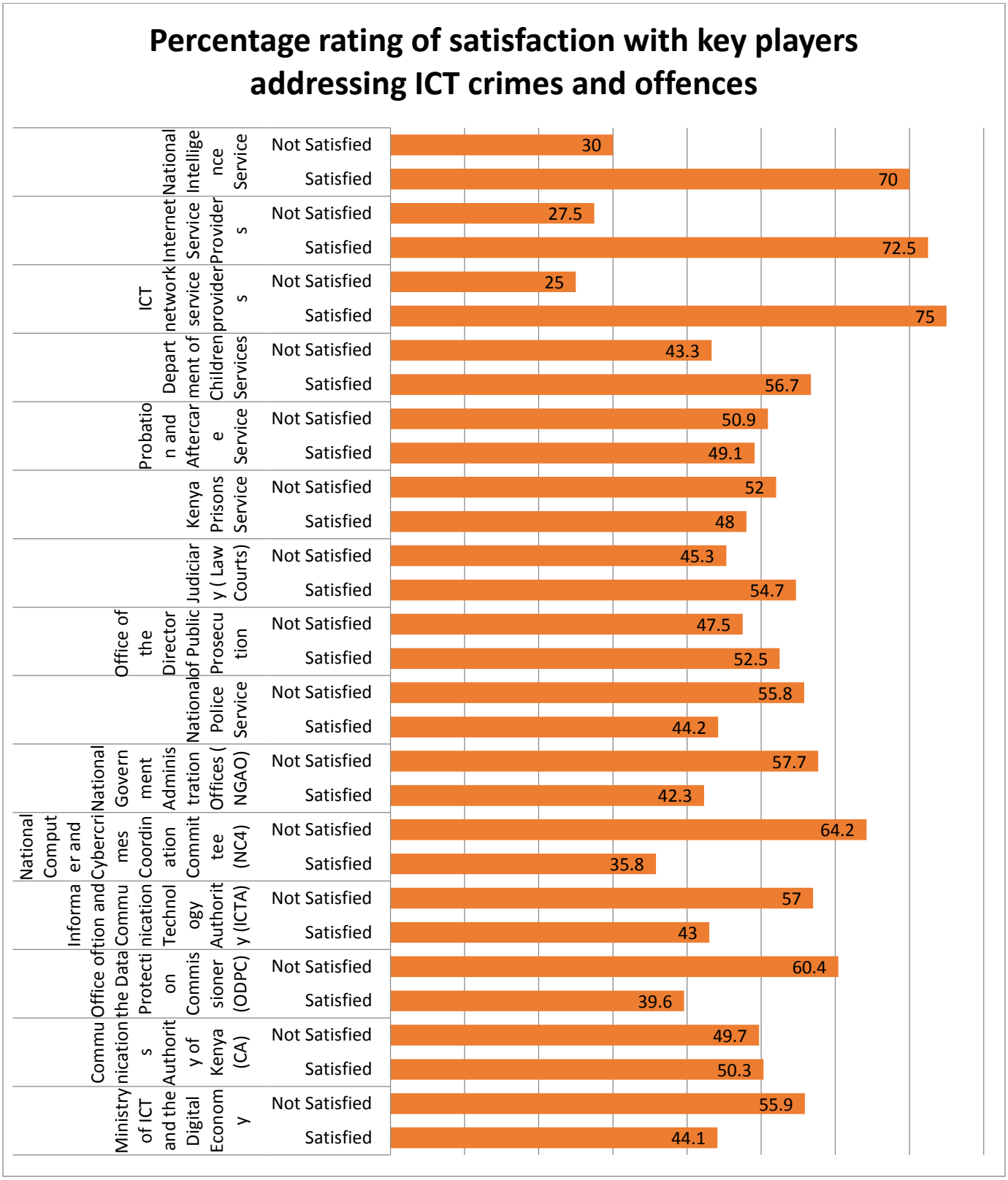
3.7.1. Satisfaction with players addressing ICT crimes and offences in Kenya

The survey results show that there is a mixed level of overall satisfaction with the efforts to address ICT crimes and offences in Kenya. From the research, (47.1%) of respondents expressed satisfaction with the efforts made by key players in addressing cybercrimes. This indicates that some initiatives and actions taken have been effective in their eyes. However, a slightly higher percentage (52.9%) of respondents expressed dissatisfaction with the service delivery related to ICT crimes and offences. This suggests that there are areas where improvements are needed to enhance the effectiveness of the measures taken. The expression of dissatisfaction by the majority of respondents highlights the urgency for improvement in the strategies, resources, and coordination among key players involved in combating ICT crimes.

There are key players involved in addressing ICT crimes and offences in Kenya, the given data shows satisfaction levels among different key players involved in addressing ICT crimes and Offences. The data indicates that satisfaction levels vary among the key players involved in addressing ICT crimes and offences. Respondents mentioned the following institutions that they were satisfied with their role in preventing ICT crimes and offences, including Communication Authority (50.3%); Office of the Director of Public Prosecutions (52.3%); Judiciary (54.7%); Department of Children (56.7%); ICT Network Service providers (75.0%); Internet Service providers (72.5%) and National Intelligence Service 70.0%. Some organizations, like ICT network service providers, internet service providers, and the National Intelligence Service had a higher satisfaction rate of over (70 %.) The data also shows institutions such as the NC4 (35.8%) and ODPC (39.4%) had lower satisfaction rates.

The data indicates that satisfaction levels vary among the key players involved in addressing ICT crimes and offences. Some organizations, like ICT network service providers and internet service providers, have higher satisfaction rates, while others, such as the NC4 (35.8%) and ODPC (39.4%), have lower satisfaction rates. Organizations with lower satisfaction rates may need to identify areas for improvement in their crime prevention measures to address the concerns of the respondents. Addressing the concerns and improving service delivery can lead to increased public trust. The satisfaction levels can highlight potential collaboration opportunities between different entities to enhance their overall effectiveness in tackling ICT crimes. The perception of the public and stakeholders about the effectiveness of these key players is crucial in maintaining public confidence and support. Key players with lower satisfaction levels can use this feedback to identify and address challenges in their crime prevention efforts. The data also indicates the importance of establishing a feedback mechanism to understand the specific concerns and grievances of the respondents and take appropriate actions to address them.

Overall, the survey results call for continuous efforts and improvements in addressing ICT crimes and offences in Kenya, with a focus on collaboration, public awareness, and the adoption of advanced cybersecurity measures. Further investigation is necessary to identify specific areas of concern that contribute to the dissatisfaction and understand the factors impacting the effectiveness of the response to ICT crimes. The findings are highlighted in Figure 11.



Source: Field data

Figure 8: satisfaction level with key players addressing ICT crimes and Offences

3.7.2. Measures addressing ICT crimes and offences in Kenya

From the survey findings, the following are the five top measures mentioned by the respondents as measures put in place to address and curb ICT crimes and offences in Kenya: Public awareness of ICT crimes and offences (74.4%) is the most widely recognized measure, with respondents acknowledging its implementation; use of strong and secure passwords, (57.2%) of respondents reported the implementation of this measure; controlled sharing of personal information, (46.7%) of respondents acknowledged the implementation of this measure; strict law enforcement, (42.3%) of respondents recognized this measure and use of ant viruses, (41.4%) of respondents reported the use of antivirus software.

Table 4: Measures addressing ICT crimes and offences in Kenya

Measures addressing ICT crimes and offences	Percent of Cases
Public awareness of ICT crimes and offences	74.4%
Use of strong and secure passwords	57.2%
Controlled sharing of personal information	46.7%
Strict law enforcement	42.3%
Use of antivirus	41.4%
Awareness of information security	39.1%
Enactment of the Data Protection Act	31.2%
Controlled access to the ICT infrastructure	29.9%
Enactment of relevant legal and policy frameworks	28.9%
Collaboration amongst the relevant stakeholders	24.7%
Use of Virtual Private Network	22.9%
Procurement of genuine software	19.9%
Introduction of multiple steps verification process	2.0%
Fresh registration of SIM card/ Verification of SIM cards	1.3%
Establishment of mentorship programs	1.2%
Creation of employment opportunities	1.2%
Use of firewalls	0.7%
Parental Control	0.6%
Tracking of lost devices	0.6%

Source: Field data

The data indicates that Kenya has taken several significant measures to address and curb ICT crimes and offences. The high level of public awareness campaigns on ICT crimes 74.4% is a positive sign, as it empowers citizens to protect themselves from cyber threats. The emphasis on strong and secure passwords, controlled sharing of personal information, and awareness of

information security best practices demonstrates a proactive approach to individual cyber hygiene. However, there is room for improvement in the implementation of certain measures. For example, the relatively lower percentages for the enactment of data protection laws (31.3%) and controlled access to ICT infrastructure (29.9%) suggest the need for further strengthening of legal and technical measures to protect sensitive data and critical systems.

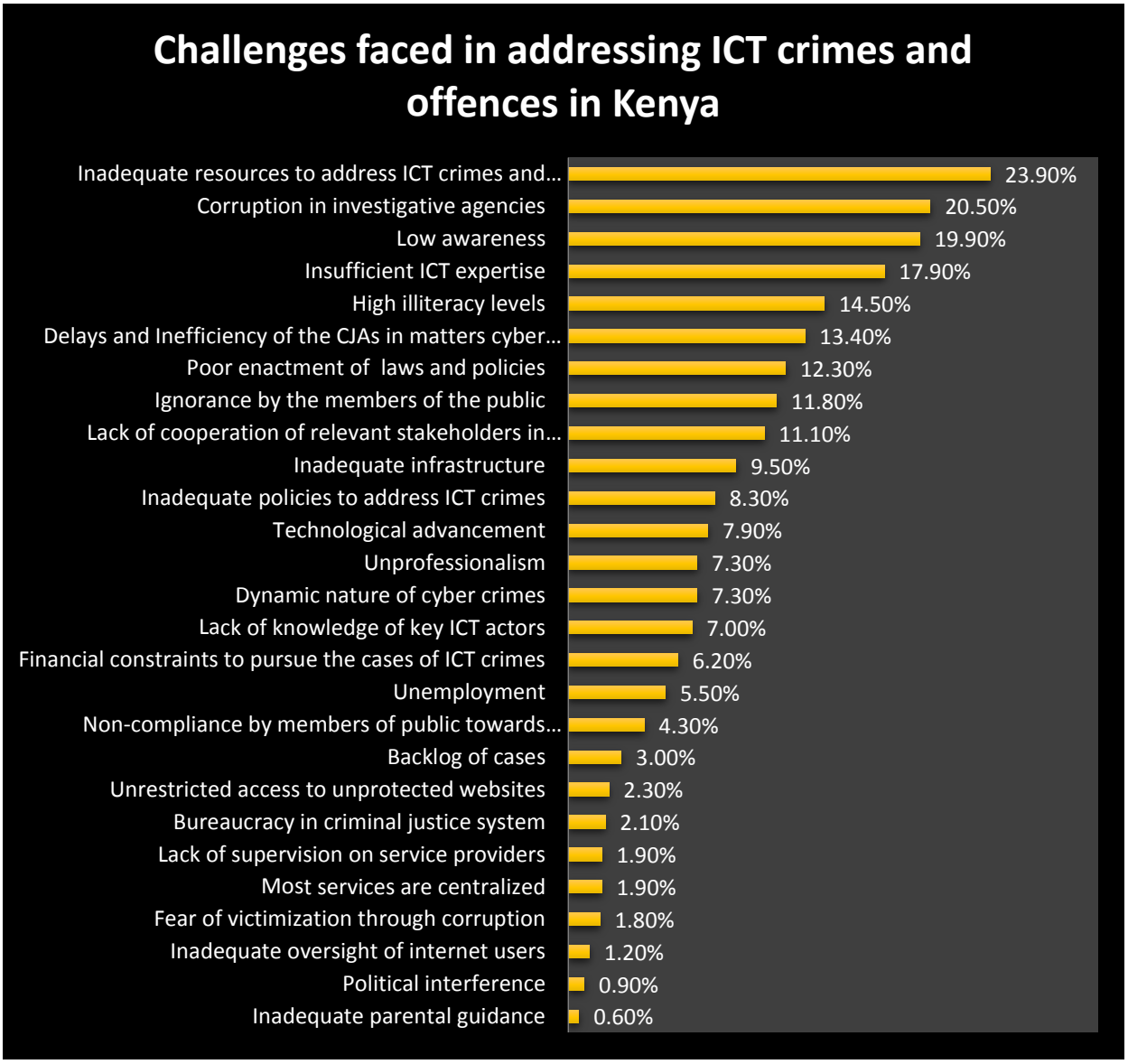
The findings also highlight the importance of collaboration among stakeholders to tackle the evolving nature of ICT crimes effectively. By working together, the government, law enforcement agencies, the private sector, and civil society can pool their expertise and resources to build a robust cyber defense ecosystem. Additionally, the low percentages for measures like the introduction of multiple steps verification process (2.0%) and establishment of mentorship programs (1.2%) suggest that there may be untapped potential in implementing these practices to enhance cyber security. Overall, the data underscores the importance of continuous efforts to improve cyber security measures, adapt to emerging threats, and create a safer digital environment for all stakeholders in Kenya.

3.8. Challenges in addressing ICT crimes and offences

The dataset underscores the primary hurdles in tackling ICT crimes and offences within Kenya. A substantial proportion of respondents indicated that a dearth of resources (23.9%) stands as the paramount challenge, followed closely by prevalent corruption in investigative bodies (20.5%), and a general lack of awareness (19.9%). Further, obstacles like a shortage of specialized ICT knowledge (17.9%), prevalent illiteracy (14.5%), and inefficiencies within the Criminal Justice System (13.4%) are also of notable concern. This information

These findings bring to light considerable impediments obstructing the path to curtailing ICT crimes and offences in the country. A shortage of essential resources, encompassing both financial and technological aspects, potentially cripples the effectiveness of law enforcement entities in both investigating and taking legal action against cybercrimes. The specter of corruption within investigative units erodes public confidence and poses a risk to the credibility and efficacy of cybercrime probes. The prevailing lack of awareness, compounded by significant illiteracy rates, amplifies the vulnerability of the populace, increasing their likelihood of being ensnared by cyber malefactors. Protracted Lengthy and inefficient procedures within the justice

system not only deny swift justice to victims but also diminish the perceived risks for would-be cybercriminals.



Source: Field data

Figure 9: Challenges faced in addressing ICT crimes and offences in Kenya

The survey's findings underscore the multifaceted strategies required to tackle the challenges of ICT crimes in Kenya. An overwhelming (74.4%) of participants stressed the importance of regular civic education programs and sensitization to equip the public with the necessary knowledge about ICT crimes, empowering them to identify and fend off cyber threats. In

parallel, nearly a quarter of respondents (24.4%) called for stricter law enforcement, signifying the need for a robust legal framework and vigorous actions against cybercriminals as a deterrent.

There is also a strong emphasis on the need for specialized training and skill development for personnel involved in handling cybercrimes, with (19.8%) of participants highlighting this as crucial. Financial support is another area of concern, with (18.6%) advocating for adequate funding for ICT regulatory agencies and (13.0%) emphasizing the need for essential equipment. Cooperation among various stakeholders, emphasized by (8.5%) of respondents, points to the necessity for a collaborative approach that pools resources and intelligence to combat intricate and evolving cyber threats effectively.

Furthermore, (12.6%) of respondents called for a review of current policies, while (5.1%) advised enacting new initiatives to adapt to the ever-changing landscape of cyber threats.

Lastly, addressing underlying issues like unemployment, which was suggested by (8.0%) of participants, could also mitigate one of the root causes of ICT crimes. The implications are clear: clear, tackling ICT crimes in Kenya requires a comprehensive, multi-pronged approach that includes education, strengthened law enforcement, professional development, adequate funding, interagency cooperation, and policy adaptation.

CHAPTER FOUR: SUMMARY OF MAJOR FINDINGS, CONCLUSION & RECOMMENDATIONS

4.1. Introduction

This chapter provides a summary of the study's major findings, which are categorized into these main thematic areas: prevalence, victims and perpetrators, institutions most affected, contributing factors, effects, satisfaction levels with institutions addressing the problem, measures put in place to address, and challenges faced in addressing ICT crimes and offences in Kenya. Additionally, the chapter offers conclusions drawn from the study and presents actionable recommendations for general stakeholders, policymakers, and institutions.

4.2. Prevalence of ICT Crimes and Offences

The study unearthed a pervasive trend of ICT crimes in Kenya. Most respondents (67.5%) rated the prevalence of ICT crimes and offences as high, indicating that these crimes are widespread and significant in Kenya. Equally, (84.8%) of respondents reported experiencing some form of ICT crimes and offences in the last 24 months, while only (15.2%) stated that they had not encountered the crimes. The three most prevalent ICT crimes reported by respondents include Computer fraud, (72.9%); identity theft and impersonation (71.5%), and interception of electronic messages or money transfers (57.3%). This isn't a minor issue but a widespread menace.

4.3. Victims and perpetrators of ICT crimes and offences

The study identified the three prominent categories of offenders committing ICT crimes and offences that include: youths, (50.1%); ICT experts (43.9%), and inmates and/or prisoners (23.1%) Various other groups, including students, hackers, and even internal staff in some institutions, have been implicated in these cyber offensives. On the receiving end, the vulnerable segments of society included the elderly (39.4%) and the uninformed (28.2%), as well as major business players (21.0%) who have borne the brunt of these crimes. This points to the need to provide requisite knowledge to people in these demographics to caution them from ICT-related crimes.

4.4. Sectors/institutions most Affected by ICT crimes

While cyber threats are universally disruptive, certain sectors feel the pinch more. The financial sector, critical in any economy, stands as a prime target, followed closely by educational institutions and the telecommunication industry. The financial sector is mostly affected by crimes and offences such as online banking fraud, credit card scams, and phishing attacks; this underscores the need for stringent cyber security measures by institutions.

4.5. Factors contributing to ICT crimes and Offences

The high incidence of Information and Communication Technology (ICT) crimes in Kenya can be attributed to various factors, as per collected data. These include economic vulnerabilities like unemployment and poverty, psychological motives such as financial greed, and societal shortcomings, including a lack of ICT literacy and the misuse of advanced technology. It's worth noting that, a significant (87.8%), of respondents identified unemployment as the major catalyst for ICT crimes. This points to the need to address the economic vulnerabilities of unemployment and poverty.

4.6. Effects of ICT Crimes and Offences

The devastating effects of Information and Communication Technology (ICT) crimes in Kenya extend well beyond the digital sphere, impacting individuals and organizations profoundly. The study findings reveal a wide range of consequences, including significant financial losses for (92.4%) of respondents; psychological distress affects (68.6%); tangible property loss (60.1%); breaches of personal information (50.5%) and data loss (46.7%). These effects pose serious security and reputation risks which further underscore the far-reaching negative impact of ICT crimes. Urgent, multi-faceted interventions are imperative to address these comprehensive and devastating consequences.

4.7. Satisfaction levels with institutions addressing ICT crimes

The survey reveals a mixed level of satisfaction regarding efforts to combat ICT crimes and offences in Kenya. While (47.1%) of respondents expressed satisfaction with the measures taken, a slightly higher percentage, (52.9%), indicated dissatisfaction, highlighting the need for

improvement in strategies, resources, and coordination among key players involved in addressing these crimes. Satisfaction levels vary among different institutions: Communication Authority, Office of the Director of Public Prosecutions, Judiciary, Department of Children, ICT Network Service providers, Internet Service providers, and National Intelligence Service garnered relatively higher satisfaction rates, exceeding (70%) in some cases. However, organizations like NC4 and ODPC had lower satisfaction ratings, indicative of the need to sensitize the public on their roles in crime prevention measures.

4.8. Measures addressing ICT crimes in Kenya

The findings of the study on key measures put in place to combat ICT crimes and offences in Kenya as reported by respondents include: Public awareness campaigns (74.4%) are the most recognized measure, empowering citizens to protect themselves from cyber threats. Emphasis on strong passwords (57.2%), controlled personal information sharing (46.7%), strict law enforcement (42.3%), and antivirus software use 41.4% demonstrates a proactive approach to individual cyber hygiene. However, there's room for improvement, particularly in enacting data protection laws (31.3%) and controlled ICT infrastructure access (29.9%) to enhance data security. Collaboration among stakeholders is crucial to effectively tackle evolving ICT crimes. Low percentages for practices like multi-step verification (2.0%) and mentorship programs 1.2% suggest untapped potential for strengthening cybersecurity.

4.9. Challenges in addressing ICT crimes and offences

The dataset highlights the significant obstacles to addressing ICT crimes and offences in Kenya. A substantial portion of respondents identified a lack of resources (23.9%) as the primary challenge, closely followed by corruption within investigative bodies (20.5%) and a general lack of public awareness of cyber crimes (19.9%). Additional hurdles include a shortage of specialized ICT knowledge (17.9%), high levels of illiteracy 14.5%, and inefficiencies within the Criminal Justice System (13.4%). These findings underscore the considerable barriers impeding efforts to combat ICT crimes.

4.10. Conclusion

This data from the Information and Communication Technology (ICT) crimes in Kenya study establishes cybercrime as a deeply ingrained and widespread problem with profound consequences for the country. The data paints a comprehensive picture, identifying the types of cybercrimes that are most prevalent, the sectors most impacted, and the demographics most affected. It also highlights those responsible for these crimes, providing a nuanced view of the actors on both sides of the law.

Notably, Kenya faces a range of challenges in tackling cybercrime. Notable among these are the lack of adequate resources, systemic corruption, a low level of public awareness, and a shortage of technical expertise. These factors collectively impede effective action against cybercrime, from its prevention to prosecution. Given these challenges, there's an urgent need for multi-faceted, collaborative solutions. Strengthening cybersecurity infrastructures, ramping up public education on cyber risks, and establishing stronger partnerships between governmental bodies, private institutions, and other stakeholders are essential steps. The research further underscores the necessity for ongoing efforts in human and technical capacity building, as well as the development and implementation of robust policies that can adapt to an ever-changing cyber landscape.

Cybercrime is a serious and evolving threat to Kenya’s national security. As technology evolves, so does the dexterity of cybercriminals, making the current preventive and corrective measures not so effective. There's a call for strengthening cybersecurity infrastructure, galvanizing public sensitization, and orchestrating harmonized efforts among various stakeholders. While the findings shed light on the grim reality, they also set the stage for rejuvenated strategies, policy revamps, and focused research. Recognizing that the digital landscape is ever-shifting, the need for ongoing vigilance, research, and adaptive responses becomes paramount. This study serves not just as an eye-opener but also as a foundational base for future academic endeavors and policy formulation aimed at creating a secure and resilient digital arena in Kenya. The actionable, data-backed recommendations laid out can act as a blueprint for ongoing and future efforts to protect the Kenyan digital landscape from the increasing threats it faces.

4.11. Recommendations of the study

4.11.1. General recommendations

1. **Strengthening Cybersecurity Infrastructure & Measures**

To enhance cybersecurity in Kenya, substantial investment is needed in cutting-edge infrastructure. The study findings established that the key challenge in addressing cybercrimes is the inadequacy of resources, about infrastructure. There is a need to employ robust measures like encryption protocols, advanced network security, and regular software updates. Additionally, critical sectors of the economy, such as healthcare, finance, and energy, should be prioritized for stringent cybersecurity protections.

2. **Public Awareness and Education**

The study findings established that Public awareness and education as the measures in place for the prevention of cybercrimes. There is a need to strengthen Civic education programs, especially targeting certain demographics like the elderly and the illiterates as the study findings established they were adversely affected by cyber-crimes. They should be rolled out to enlighten the public about safe online practices, including the use of strong passwords and avoiding phishing attempts. This education should extend to schools and universities, incorporating cybersecurity topics into the standard curriculum. Targeted campaigns, focusing on vulnerable groups like children can further tailor the awareness efforts.

3. **Law Enforcement, Capacity Building, and Prosecution**

The capacity of law enforcement agencies and the judiciary needs strengthening to effectively combat cybercrimes. The study findings established the prevalence of high-tech *modus operandi* by cyber criminals such as hacking, phishing, and social engineering, this indicates the need for heightened cyber security through specialized training programs in cyber investigations, digital forensics, and the prosecution of cybercrimes. There should also be enhanced inter-agency coordination to ensure that cybercrime cases are efficiently handled and brought to a conclusion, sending a strong signal of zero tolerance against cyber offenders.

4. **Policy Revisions, Regulation, and Legislation**

The legal framework governing cyber security in Kenya requires periodic review and updating. This would help to close existing legal loopholes and adapt to the evolving nature of cyber threats. Sector-specific guidelines should be implemented, tailored to the unique challenges faced by sectors like finance, healthcare, and education which were some of the highly affected sectors as per the study findings. Introducing stringent penalties for cybercriminal activities can serve as a significant deterrent.

5. **Collaboration, Cooperation, and Information Sharing**

Combating the findings also highlights the importance of collaboration among stakeholders to tackle the evolving nature of ICT crimes effectively. Combating cyber threats is a collective effort that requires strong cooperation among government agencies, the private sector, civil society, and international partners. Platforms for efficient information sharing should be created to enhance the collective intelligence around cyber threats. International cooperation is crucial for tackling the transnational nature of many cyber threats.

6. **Resource Allocation and Funding**

One of the challenges of addressing cyber security is the inadequacy of resources, both financial and technological. The study findings established that proper funding of regulatory agencies addressing ICT crimes could help in dealing with cyber security. Funding should be directed toward the acquisition of modern technological tools and infrastructure that can strengthen cybersecurity efforts. Research and development in cyber security should also be financially supported to foster innovation.

7. **Monitoring, Reporting, and Response**

Real-time monitoring and early warning systems are essential for the early detection of cyber threats. User-friendly reporting channels should be established to encourage prompt reporting of cyber incidents. A dedicated National Cyber Security Incident Response Team (CSIRT) should be set up to coordinate immediate and effective responses to cyber threats and incidents.

8. Public-Private Partnerships

Public-private partnerships can serve as a cornerstone for a resilient cybersecurity ecosystem. Businesses should be encouraged to adopt cyber insurance policies, and a certification system can be implemented to ensure that organizations meet minimum cyber security standards. These partnerships can serve to share best practices and bolster overall national cyber security.

9. Job Creation and Youth Empowerment

Addressing underlying issues like unemployment can reduce the appeal of cybercriminal activities. Job creation, particularly in the ICT sector, and youth empowerment programs can serve as preventive measures. Skill development initiatives can equip young people with the right tools to engage in ethical digital behavior.

10. Data Protection and Privacy

Data protection and privacy laws should be strengthened to safeguard the personal information of Kenyan citizens. Stricter regulations should be imposed on organizations and service providers to ensure the highest standards of data protection. Mechanisms for the prompt reporting and addressing of data breaches should be institutionalized.

4.11.2. Institutions recommendations

A. Regulatory and Law Enforcement Agencies

a) **Collaborative Enforcement:** Intensify multi-stakeholder collaborations and adopt a zero-tolerance policy against cyber offenders.
b) **Expertise Development:** Allocate resources for specialized training of personnel engaged in cybercrime control, ensuring they are updated on the latest investigation techniques.
c) **Incident Reporting:** Develop streamlined reporting channels to expedite the identification and neutralization of cyber threats.
d) **Regulatory Rigor:** Vigorously apply existing cybersecurity laws to set a deterring precedent for potential offenders.

e) **Specialized Cyber Units:** Establish dedicated departments within law enforcement focused solely on cybercrime probes and litigation.
f) **Inter-agency Coordination:** Promote synergy among governmental bodies, the private sector, NGOs, and international allies for an integrated anti-cybercrime strategy, including joint response teams for improved information sharing.
g) **Judicial Efficiency:** Reform and prioritize cybercrime in the legal process, advocating for inter-agency collaboration for swift prosecution.

B. ICT Regulatory Agencies

a) **Resource Allocation:** Amplify the funding of ICT regulatory bodies for the procurement of cutting-edge cyber security technology.
b) **Public Awareness:** Regularly run civic education programs detailing cyber security threats and preventive measures.
c) **Community Outreach:** Partner with educational institutions, media, and community leaders to broaden cybercrime awareness.
d) **Policy Revamp:** Periodically review and update existing ICT policies to adapt to the evolving cybersecurity landscape

C. Financial Sector

a) **Security Protocols:** Mandate the usage of multi-factor authentication for transactions.
b) **Infrastructure Security:** Invest in advanced cyber security solutions like strong firewalls and antivirus software.
c) **Employee Training:** Regularly update staff on cyber security best practices through dedicated training sessions.
d) **Data Protection:** Enforce rigorous compliance with data protection legislation to guard against data leaks.

D. Educational Institutions

a) **Curriculum Integration:** Incorporate cyber security basics into the academic curriculum to foster digital responsibility.
b) **Community Education:** Hold regular seminars and workshops to inform the general populace about the risks and countermeasures associated with ICT crimes.
c) **Research & Development:** Encourage academic-industrial-governmental partnerships to innovate new cybersecurity solutions.

E. Telecommunication Sector

a) **Identity Verification:** Strengthen SIM card registration processes to minimize anonymous and malicious usage.
b) **Collaborative Defence:** Actively cooperate with law enforcement and governmental agencies to share vital intelligence against cyber threats.
c) **Data Safeguarding:** Ensure uncompromising adherence to data protection standards to prevent unauthorized data access.
d) **Consumer Education:** Encourage end-users to adopt robust cybersecurity practices, like strong passwords, two-factor authentication, and frequent software updates.

4.12. Recommendations for Further Research

While this study offers a comprehensive exploration of Information and Communication Technology (ICT) crimes in Kenya focusing on prevalence, affected demographics, the key factors involved, the underlying drivers, consequences, and current countermeasures, it also reveals gaps that warrant further investigation. The following areas are proposed for subsequent research endeavors:

1. **Assessing Government Cyber Security Preparedness:** Although this study collected experiential data from government employees, it did not directly scrutinize the readiness of government institutions to counter cyber threats. Future research should delve into the vulnerabilities and preparedness levels of these agencies. Such assessments are critical not just for national security, but also for the safeguarding of citizen data, sustaining public trust, and ensuring economic resilience.

2. **Evaluating Policy Efficacy:** This study examined existing countermeasures but did not focus on the policy and regulatory framework in place. Subsequent research should assess the effectiveness of current cyber security policies, using data-driven analyses to inform more robust and flexible policy initiatives. Such an approach would help identify lacunae in current frameworks and propose informed solutions.
3. **Security Concerns in Emerging Technologies:** The rapid proliferation of technologies like Artificial Intelligence, the Internet of Things, and 5G networks exposes new vulnerabilities. These technologies are becoming integrated into critical sectors like healthcare, finance, and energy, raising concerns about the potential for cyber attacks. Future research must assess the security ramifications of these technologies, aiming to inform proactive measures for securing our digital future.
4. **Socioeconomic Factors and Cybercrime:** This study identified that economic vulnerabilities, particularly among the youth, were a significant driver of ICT crimes. A dedicated research initiative should explore the link between socioeconomic conditions such as unemployment and poverty, and the rise in cybercrime. Such a study could aid policymakers in creating targeted, effective interventions like skills training programs or job creation in tech-related sectors.

By exploring these areas, future research can build on the insights of this study, providing a more nuanced and complete understanding of the cybercrime landscape in Kenya. This will support the development of well-rounded, data-driven strategies and interventions to protect Kenya's digital ecosystem.

REFERENCES

AFP. (2010, 12 March). Cybercrime surge pushes 2009 losses to 559 million dollars. Retrieved 30 August 2022, from http://www.france24.com/en/20100312-cybercrime-surge-pushes-2009-losses-559-mi million-dollars

AsherryMagalla (Jan 1, 2018). Prevention and Detection of Cyber Crimes in Tanzania as Described by Cyber Crime Act.

Arneklev, B. J., Harold, G. G., Tittle, C. R., Bursik, R. J. (1993). Low self-control and imprudent behavior. Journal of Quantitative Criminology, 9, 225–247.

ERenErsozoglu (April 15th 2021). Cyber Crime in East Africa. Retrieved on 13August 2022 from https://greydynamics.com/transnational-organised-crime-in-east-africa-cyber-crime/

Kshetri, Nir (2019). "Cybercrime and Cybersecurity in Africa," Journal of Global Information. Technology Management. DOI: 10.1080/1097198X

Ochieng A (2019) Focus on awareness as Kenya's cyber threats jump to 135pc. Business Daily, accessed on 19/08/2022 from https://www.businessdailyafrica.com/datahub/Focus-on-awareness–as-Kenya–threats-jump/3815418-5292602-4n0mhb/index.html

Owaida A (2020) Technology is getting Smarter are we, accessed on 19/08/2022 from https://www.welivesecurity.com/2019/12/10/cybersecurity-trends-2020-technology-is-getting-smarter-are-we/

Roderic Broadhurst& Yao-Chung Chang (2012). Cybercrime in Asia: trends and challenges. Retrieved 31 August 2020 from https://www.researchgate.net/publication/256028676_Cybercrime_in_Asia_Trends_and_Challenges/citation/downloadhttps://surfshark.com/research/data-breach-impact/statistics Retrieved on 30 August 2020

Gottfredson, M., &Hirschi, T. (1990). A General Theory of Crime. Stanford, CA: Stanford University Press Retrieved on 3 August 2022 https://www.scirp.org/reference/ReferencesPapers.aspx?ReferenceID=1315907

Rogers, S. (2006). Evidence-Based Interventions for Language Development in Young Children with Autism. In T. Charman& W. Stone (Eds.), Social & Communication Development in Autism Spectrum Disorders: Early Intervention, Diagnosis, & Intervention. (pp.143 – 179). New York: Guilford Press.

Pratt et al. 2014; Schrek, 1999) Self- control and victimization: A meta- analysis

Symantec. (2018). Internet Security Threat Report.

Ngo, F., &Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. International Journal of Cyber Criminology, 11(1), 1-9.

Jaishankar, K. (2007). Cyber Criminology: Evolving a Novel Discipline with a New Journal. International Journal of Cyber Criminology, 1(1), 1-6

Grabosky, P., & Smith, R. (2017). Cybercrime. In D. Palmer, W. de Lint, & D. Dalton (Eds.), Crime and Justice: A Guide to Criminology (5th ed., pp. 243-277). Sydney, Australia: Thomson Reuters (Professional) Australian Limited.

Grabosky, P. (2004). The Global Dimension of Cybercrime. Global Crime, 6(1), 146- 157.

Gibson, W. (1995). Neuromancer. London: Harper Collins Publishers.

Internet World Stats. (2018). World Internet Users and 2018 Population Stats. The Big Picture

Serianu (2018) Africa Cyber Security Report-Kenya, accessed on 19/08/2022 from https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

Stephen Chege (2021). Uganda: Shs15b Was Lost Through Cyber Fraud Last Year, The Monitor 15th July 2021.

US Internet Crime Complaints Centre, (2020). Global Cybercrime Report

Wainaina W (2019) Surge in cyber-attacks presents new opportunities for insurers, accessed on 19/08/2022 from https://www.standardmedia.co.ke/business/article/2001341416/surge-in-cyber-attacks-presents-new-opportunities-for-insurers

APPENDICES

Appendix I: Interview Schedule/Questionnaire

INFORMATION COMMUNICATION TECHNOLOGY CRIMES AND OFFENCES IN KENYA

County: _____
Sub-County: _____
Division: _____
Location:_____
Date of interview: _____
Start time: _____ End Time: _____
Name of the Researcher: _____

Introduction

The **National Crime Research Centre** (NCRC) is a State Corporation under the Ministry of Interior and National Administration established by the National Crime Research Centre Act No. 4 of 1997. The Centre is conducting an assessment of Information Communication Technology (ICT) crimes and offences in Kenya to inform relevant policies and programs.

All the information you give will be treated with utmost confidentiality and your identity will not be revealed. We would highly appreciate it if you spared some time to respond to the following questions.

Respondent consent Yes ( ) No ( )

Institution of Affiliation_____

Section A: Respondent's Socio-demographic Information

1. Gender:
1. Male
2. Female

2. Age of respondent in years

1. 18-34
2. 35-51
3. 52-68
4. 69+

3. Marital Status

1. single/Never married
2. Married
3. Separated
4. Divorced
5. Widowed

4. Highest level of education

1. None
2. Primary
3. Secondary
4. Middle Level College
5. University
6. Adult Literacy
7. Others (specify) _____

5. Main Occupation

1. Permanent employment-Private Sector
2. Permanent employment- Public sector
3. Casual/temporary employment
4. Business person
5. Other(specify)_____ _____

Section B: Types and prevalence of ICT crimes and offences

6. (a) In general, based on your knowledge, how would you rate the prevalence of ICT crimes and offences in Kenya?

1. High
2. Medium
3. Low

(b) Based on your knowledge and/or experience, which sectors and/or institutions have been most affected by ICT crimes and offences in Kenya?

_____

_____

(c) Based on your knowledge and/or experience, please list ICT crimes and offences that are prevalent in Kenya.

S/No.	ICT crimes and offences that are prevalent	Tick all that apply (✓)
1.	Child pornography	
2.	Publication and false information	
3.	False publication	
4.	Computer forgery	
5.	Computer fraud	
6.	Cybersquatting	
7.	Identity theft and impersonation	
8.	Phishing	
9.	Interception of electronic messages or money transfers	
10.	Wilful misdirection of electronic messages	
11.	Inducement to deliver an electronic message	
12.	Intentionally withholding messages delivered erroneously	
13.	Unlawful destruction of electronic messages	
14.	Wrongful distribution of obscene or intimate images	
15.	Fraudulent use of electronic data	
16.	Unauthorized access	

S/No.	ICT crimes and offences that are prevalent	Tick all that apply (✓)
17.	Access with intent to commit further offence	
18.	Unauthorized interference	
19.	Unauthorized interception	
20.	Illegal devices and access codes	
21.	Unauthorized disclosure of password or access code	
22.	Offences involving protected computer system	
23.	Cyber espionage	
24.	Issuance of false information	
25.	Subversion	
26.	Cyber harassment	
27.	Cyber terrorism	
28.	Aiding and abetting crime	
29.	Offences by a body corporate and limitation of liability	
30.	Failure to report cybercrime within 24 hours	
31.	Failure to relinquish access codes	
32.	Others (specify)	

7. (a**)** Have you/ or anyone you know experienced any form of ICT crimes and offences in the last 24 months?

1. Yes 2. No

(b**)** If yes in Q7 (a), which are the ICT crimes and offences experienced in the last 24 months?

S/No.	ICT crimes and offences experienced in the last 24 months	Tick all that apply (✓)
1.	Child pornography	
2.	Publication and false information	
3.	False publication	
4.	Computer forgery	
5.	Computer fraud	
6.	Cybersquatting	
7.	Identity theft and impersonation	
8.	Phishing	
9.	Interception of electronic messages or money transfers	
10.	Wilful misdirection of electronic messages	
11.	Inducement to deliver an electronic message	
12.	Intentionally withholding messages delivered erroneously	
13.	Unlawful destruction of electronic messages	
14.	Wrongful distribution of obscene or intimate images	
15.	Fraudulent use of electronic data	
16.	Unauthorized access	
17.	Access with intent to commit further offence	
18.	Unauthorized interference	

S/No.	ICT crimes and offences experienced in the last 24 months	Tick all that apply (✓)
19.	Unauthorized interception	
20.	Illegal devices and access codes	
21.	Unauthorized disclosure of password or access code	
22.	Offences involving protected computer system	
23.	Cyber espionage	
24.	Issuance of false e-information	
25.	Subversion	
26.	Cyber harassment	
27.	Cyber terrorism	
28.	Aiding and abetting crime	
29.	Offences by a body corporate and limitation of liability	
30.	Failure to report cybercrime within 24 hours	
31.	Failure to relinquish access codes	
32.	Others (specify)	

Section C: Perpetrators and victims of ICT crimes and offences

8. Based on your knowledge and/or experience, who are the main perpetrators of ICT crimes and offences in Kenya?

_____

_____

9. Based on your knowledge and/or experience, who are the main victims of ICT crimes and offences in Kenya?

_____

_____

10. Based on your knowledge and/or experience, how are ICT crimes and offences committed?

_____

_____

Section D: Factors Contributing to ICT crimes and offences

11. Based on your knowledge and/or experience, what are the factors contributing to ICT crimes and offences in Kenya?

S/No	Factors contributing to ICT crimes and offences	Tick all that apply (✓)
1.	Vulnerability occasioned by unemployment or underemployment	
2.	Vulnerability occasioned by poverty	
3.	Illiteracy on ICT matters	
4.	Ignorance of cyber security measures	
5.	Financial greed	

S/No	Factors contributing to ICT crimes and offences	Tick all that apply (✓)
6.	Infiltration for fun	
7.	Inadequate cyber security measures	
8.	Negative peer influence	
9.	Rivalry and competition	
10.	Abuse of technological advancement	
11.	Others (specify)	

Section E: Effects of ICT crimes and offences

12. Based on your knowledge and/or experience, what are the effects of ICT crimes and offences in Kenya?

S/No.	Effects of ICT crimes and offences	Tick all that apply (✓)
1.	Breach of privacy	
2.	Financial loss	
3.	Loss of property	
4.	Imprisonment	
5.	Moral distortion	
6.	Loss of lives	
7.	Psychological distress	
8.	Manipulation from unguarded information	
9.	Blackmail	
10.	Online violence and abuse	
11.	Hatred	
12.	Denial of service	
13.	Reputation damage	
14.	Loss of employment	
15.	Loss of data	
16.	Others (specify)	

13. (a) Based on your knowledge and/or experience, who are the key players involved in addressing ICT crimes and offences in Kenya?

S/No.	Key players involved in addressing ICT crimes and offences (Regulatory/Law Enforcement/Service providers	Rating of your satisfaction with crime prevention measures (Please tick your choice)	
		Satisfied	Not satisfied
1.	Ministry of ICT and the Digital Economy		
2.	Communications Authority of Kenya (CA)		
3.	Office of the Data Protection Commissioner(ODPC)		
4.	Information and Communication Technology Authority (ICTA)		
5.	National Computer and Cybercrimes Coordination		

	Committee (NC4)		
6.	National Government Administrative Offices		
7.	National Police Service		
8.	Office of the Director of Public Prosecutions		
9.	Judiciary (Law Courts)		
10.	Kenya Prisons Service		
11.	Probation and Aftercare Service		
12.	Department of Children Services		
13.	Others (specify)		

(b) Based on your knowledge and/or experience, what measures have been put in place to address/curb ICT crimes and offences in Kenya?

S/No	**Measures that have been put in place to address/curb ICT crimes and offences**	**Tick all that apply (✓)**
1.	Public awareness of ICT crime and offences	
2.	Controlled access to the ICT infrastructure	
3.	Use of Anti-Viruses	
4.	Enactment of relevant legal and policy frameworks	
5.	Strict law enforcement	
6.	Collaboration amongst the relevant stakeholders	
7.	Awareness of information security	
8.	Use of strong and secure passwords	
9.	Use of virtual private network	
10.	Procurement of genuine software	
11.	Controlled sharing of personal information	
12.	Enactment of the Data Protection Act	
13.	Others (specify)	

Section F: Challenges faced in addressing ICT crimes and offences and Recommendations

14. (a) What are the challenges faced in addressing ICT crimes and offences in Kenya?

_____

_____

(b**)** What would you recommend be done to address challenges faced in tackling ICT crimes and offences in Kenya?

_____

_____

*** Thank you for your cooperation**

Appendix II: Key Informant Interview Guideline Questions

INFORMATION COMMUNICATION TECHNOLOGY CRIMES AND OFFENCES IN KENYA

County: _____
Sub-County: _____
Venue: _____
Date of the survey:_____
Start time: _____ End Time:_____
Name of the Research Assistant: _____

The **National Crime Research Centre** (NCRC) is a State Corporation established by the National Crime Research Centre Act (CAP, 62 LoK). The Centre is conducting an assessment of information communication crimes and offences in Kenya. All the information you give will be treated with utmost confidentiality and your identity will not be revealed. We would highly appreciate it if you spared some time to respond to the following questions.

Respondent consent Yes ( ) No ( )

1. What are the ICT crimes and offences that are prevalent in this locality?
2. Who are the perpetrators and victims of ICT Crimes and offences?
3. What are the factors contributing to ICT Crimes and offences?
4. What are the control measures that individuals have taken to protect themselves from ICT crimes and offences?
5. What measures have regulatory agencies and service providers taken to protect people from ICT crimes and offences?
6. What are the effects of ICT crimes and offences?
7. What challenges do the ICT players face in addressing the ICT crimes and offences?

8. What are the weaknesses of the control measures in place in addressing ICT crimes and offences?
9. In your opinion, what are the ways they can address these challenges

*** Thank you for your cooperation ***

NATIONAL CRIME RESEARCH CENTRE
ACK Garden Annex - Ground Floor
1st Ngong Avenue, Off Bishop's Road
P.O. Box 21180-00100 Nairobi, Kenya
Tel: Tel: +254-20-2714735/0722 980 102
Email: director@crimeresearch.go.ke
Website: www.crimeresearch.go.ke