**NATIONAL DEFENCE UNIVERSITY- KENYA (NDU-K)**
**NATIONAL DEFENCE COLLEGE (NDC)**

# INFORMATION SECURITY THREATS TO E-GOVERNMENT SERVICES IN KENYA

**BY**

**GODFRED OHNDYL OTIENO**

**ADM NO ND601/0013/2022**

**SUPERVISOR: COL (DR) JAMES J KIMUYU (PhD)**

**A thesis submitted in partial fulfilment for the award of Maters of Arts in National Security and Strategy**

**May 2023**

## DECLARATION

This project is my own original work and to the best of my knowledge it has not been presented for examination to any other university for any other award.

Signature: ..... Date 28/04/2023

GODFRED OHNDYL OTIENO

**Supervisor's Approval**

This project has been submitted for examination with my approval as university supervisor.

Signature..... Date 28.04.2023

COL (DR) JAMES J KIMUYU (PhD)

## DEDICATION

I dedicate this research project to my wife Esther and children Stephanie, Lincoln, Victoria and Yosef for their selfless love and support during the period of my National Defence College studies.

## ACKNOWLEDGEMENT

I would like to acknowledge the Kenya Defence Forces(KDF), the National Defence University – Kenya(NDU-K) and the National Defence College(NDC) for giving me this opportunity to undertake this master's course. I sincerely give my gratitude to my able supervisor Col (Dr) James Kimuyu (PhD) for his final guidance on the thesis. My recognition further extends to my fellow course mates, the entire academic and support staff that worked under the Programme. Again my thanks go to my Commanders, Officers and Airmen at the Kenya Air Force for their continued inspiration to complete the studies. Much gratitude to Mollie Margaret for her tireless editorial support.

To all of the aforementioned, I say may God bless you abundantly.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

AfCFTA - African Continental Free Trade Area

AI - Artificial Intelligence

AP - African Passport

AU - African Union

CFI - Continental Financial Institution

GIDI - Global Innovation Development Index

GST - General System Theory

ICT - Information Communications and Technology

IGO - International Governmental Organization

IT - Information Technology

ITN - Integrated Transport Network

MDG - Millennium Development Goals

MTP - Medium Term Plan

NACOSTI - National Commission of Science, Technology and Innovation

NDU-K - National Defence University –Kenya

PAEN - Pan African E-Network

PVA - Pan African Virtual University

R&D - Research and Development

SDG - Sustainable Development Goals

SPSS - Statistical Package of Social Science

SSA - Sub - Sahara Africa

STI - Science, Technology and Innovations

UN - United Nations

## ABSTRACT

This study examined the information security threats to e-government services commonly known as the e-citizen services in Kenya. Globally, governments are increasingly losing control and sovereignty over the cyberspace to other states, non-state and individual actors competing for various forms of power with varying intentions. This is due to increased interconnected and interdependency on integrated internet service enabled digital communication infrastructures. The specific objectives were types of public services, types of information security threats and identification of security measures required to protect safety, access, integrity, confidence and privacy of efficient and effective e-government services. The study used descriptive research design adopting mixed method cross sectional survey. The target population was 12000 respondents from 51 Huduma Centres countrywide. Purposive sampling at 10% was chosen where 1200 questionnaires were issued which returned 966 responses at 80%. The study applied both quantitative and qualitative analysis using Statistical Package of Social Science (SPSS) data processing software. Hypothesis testing at 5% significance level. The research findings are presented in tables, figures, graphs and descriptive statistics. The study found that Kenyan citizens were the majority users at 50%, Kenyan registered Companies at 35%, Foreign Agencies 10% and Foreign Citizen individuals at 5%. The services sought; Government to (G2C) 43%, Government to Business (G2B) 35%, Government to employees (G2E) 20% and Government to Government (G2G) 2%. The hypothesis test for the quality of services, $Chi^2$ –Test = $x^2$ , df 3 (n-1) = $\sum (Oi - Ei)^2 / Ei = 10.83 > 9.35$ at 5% significantly greater. The study identified 13 categories of cyber security threats i.e unauthorized access, illegal devices, unauthorized codes, false publications, computer frauds, cyber espionage, terrorism and squatting, phishing, identity thefts, electronic interceptions, fraudulent electronic data, employee aiding, child pornography and others. The hypothesis test for information security threats, $Chi^2$ –Test = $x^2$ , df 11 (n-1) = $\sum (Oi - Ei)^2 / Ei = 20.47 > 19.68$ at 5% significantly greater. The study further identified 10 categories of security measures i.e Legislations, institutional policies, capacity development training, backups, physical access, professional certification, frequent ICT audits, firewalls and management security reviews. The hypothesis test for the preventive measures, $Chi^2$ –Test = $x^2$ , df 9 (n-1) = $\sum (Oi - Ei)^2 / Ei = 18.39 > 16.92$ at 5% significantly greater. The study recommends strongly development of home country made technologies and critical infrastructure, international cyber security collaboration, frequent infrastructure security audits, monitoring and upgrades, employee and user capacity training and institutional critical equipment and infrastructure reviews and restructuring of national security organs to create cyber space capabilities to guarantee preventive, defensive and offensive capabilities in tandem to the evolving global information security threats and increasing geopolitical competition and rivalries.

# CHAPTER ONE: INTRODUCTION

## 1.0 Introduction

This study examined the information security threats to e-government services in Kenya in an increasingly volatile, uncertain, complex and ambiguous operating environment where national sovereignty and independence faces a number of threats from the cyber security space. The globalization and advancements in information and communication and technology has caused increased connectivity and interdependency of the world systems. Governments, business organizations and citizens have embraced technology in provision of services. The Kenya government adoption of electronic services occurs in an increasingly uncertain environment facing significant security threats to the nations.

The vision 2030, seeks to make Kenya a newly industrializing middle income knowledge based economy providing high quality life to all citizens by the year 2030. The implementation of this blue print focusses on three pillars; the economic, political and social pillars which gives heavy weight on the development of Information Communications and Technology (ICT) as an enabler towards achievement of this vision. Vision 2030 blue print is being implemented on a five year Medium Term Plan (MTP) basis, currently on third term of implementation. This study asses the status, progress and challenges made within the (ICT) sector. It examines information security threats facing exponential growth in digital transformation process in the highly globalizing operating environment with no definite physical boundaries.

## 1.1 Background of Study

The digital transformation and applications within the ICT industry has been quite astronomical within the 21st Century, and so has been the risks, challenges and opportunities that have come along. The advancement in computing technologies, communications protocols, information processing, programming, telecommunications, aerospace, satellite, electronics, chips, artificial intelligence (AI), communications, avionics, electrical, power and fiber optics have in overall revolutionized modernization and thus globalisation of the world production, manufacturing, service, markets and public organization. [1]

The advanced countries have continued to lead in scientific and technological inventions, innovations and economic exploitation of ICT in the conduct of business, commerce, trade and social life. However, the developing countries particularly in the Sub - Sahara Africa (SSA) still lag behind due to poor economies, low penetration level of technology, high asset acquisition costs, lack of infrastructure and largely poor and illiterate populations. This poor performances also affect some countries in parts of Latin America and East Asia.[2]

In 2015, the United Nations (UN) rolled out the Agenda 2030 for sustainable development of the world following the achievement of the earlier strategy of the Millennium Development Goals (MDGs). The International Governmental Organization

[1] Kremling, Janine., Amanda, M., Sharp Parker. Cyberspace, Cybersecurity and Cybercrime. (London: SAGE Publications, 2018), 110.
[2] Rose, Farina. Securing what you don't own or have. (Washington DC: Oxford University Press, 2019), pp.230-232.

(IGO), launched seventeen other agendas popularly known as the Sustainable Development Goals (SGDs). The aims of these goals are to improve lives of world population by the year 2030. Key among these objectives are; Elimination of poverty, improved quality education, access to affordable and clean energy, access to decent work and sustained economic growth, increased industry, infrastructure and innovations, sustainable cities and societies, responsible consumption and production, advanced life on land, build global partnership among many others.[3] All these initiatives embraces the development of world knowledge economy frame worked on ICT.

The UN through policy support initiatives has equally encouraged states to embrace digital economies. The 2020 UN E-Government Survey observes tremendous efforts by various government in response to the influence of COVID-19 Pandemic that accelerated the implementation of e-governance programmes.[4] At the continental level, the African Union (AU) Agenda 2063 framework, further seeks to consolidate the social-economic transformations of the continent. This African policy initiative mirrors largely on the UN SDGs.

The policy agenda item that speaks to the focus of this study is the development of human capital, social assets, infrastructure and public goods. This sector has attracted major flagship programmes for implementation in e-governance; Integrated Transport Network (ITN), African Continental Free Trade Area (AfCFTA), Pan African E-Network (PAEN), African Passport (AP), Pan African Virtual University(PVU) and Continental

[3] UN SDG (2015), https://unstats.un.org/sdgs, Accessed on 20th August 2021.
[4] UN E-GOVERNMENT SURVEY (2020), publicadministration.un.org, Accessed on 20th August 2021.

Financial Institution (CFI) on integrated approach basis. This continental strategy seeks to establish a strong digital foundation for enhanced continental economic growth and inclusiveness within the continent.[5] This will further be enabled through the ICT platform as a stimulant and as an enabler.

At the local level, Kenya remains focused on enhancing growth of digital knowledge based economy. The Kenya constitution 2010 vests sovereign power in the citizens and provides the legal policy framework for progressive democratic governance embracing effective service delivery, transparency and accountable leadership.[6] The government has thus rolled out partial e-governance strategies and programmes embracing developments in both Science, Technology and Innovation (STI) and Information, Communication and Technology (ICT) sectors. These will speed up national transformations towards digital knowledge economy which is an important ingredient of Kenya's industrialization.[7]

The Kenya e-governance initiatives focuses on; e-tax, e-customs, one-border stop, e-citizen, e-passport, e-cities, e-health, among many other public services to be offered within central government and county devolved units. These saw the establishment of Huduma Centres in major towns for easy access of public services by the citizens. The government, leading telecommunication companies, banking institutions, citizens and other stakeholders have largely accepted and embraced modern technology in the conduct of official business making it easier for adoption and implementation of integrated digital

[5] AU AGENDA 2063 (2015), https://au.int/en/agenda2063/overview, Accessed on 20th August 2021.
[6] Government of Kenya, The Constitution, 2010, http://kenyalaw.org/kl/index.php?id=398. Accessed on 14 August, 2022 at 1130 pm.
[7] Government of Kenya, Vision 2030 (2015), https://vision2030.go.ke/, Accessed on 20th August 2021.

services. This has further been made possible through the easy availability of cheap and affordable mobile telephone and computer devices, infrastructure expansion and internet connectivity.[8] This successes are happening within a globalizing world that is already attracting security threats within the largely declining national sovereignty environment bring along ICT based threats arising from the global network connectivity.[9]

The number of businesses that have experienced data breaches has grown exponentially during this 21st Century. The number of recorded cases and financial loses have risen enormously. Illustrating the scope and potential severity of this issue are examples like the 2017 Equifax data breach that affected almost 148 million individuals and the 2013 Yahoo breach that affected three billion individuals globally. Similarly, a hacker accessed 106 million of Capital One's credit card customer and applicant accounts in March 2019.[10] For a government, the cost of data breaches can be significant. This study thus seeks to examine information security threats to e-government services in Kenya with the purpose of establishing appropriate security measures against the challenges.

## 1.2 Statement of Research Problem

Globalisation has been characterized by astronomical advances in Information, Communication and Technological (ICT) domain. These high value technological development have fundamentally revolutionized the conduct of international trade and

[8] KNBS, ICT SURVEY (2016), 5.
[9]Ciampa, M. Security Awareness ( Boston:, MA Cengage, 2018) , 75.
[10] Clement, Annual data breaches, (2019, ). Pp. 26-32.

commerce and delivery of public services by modern nation states.[11] This new developments have been accompanied by information security management challenges to guarantee safety of data, accessibility, integrity, confidentiality and privacy. Some of these challenges includes cybercrime, economic crimes, transnational crimes, systems and infrastructure intrusions, data fraud, equipment destruction, denial and disruption of services.[12] The growth and proliferation of Artificial intelligence and destructive digital technologies continue to increase ideological competition among the world superpowers and emerging great powers. This has witnessed opening of new cyber warfare domains and military defence restructuring capabilities to guarantee preventive, defensive and offensive capabilities within the cyber space.[13] Developing nations such as Kenya and mostly the fifth world nations face severe capability development challenges in the acquisition, adoption, use and management of data in the new global digital economy and infrastructure.[14]

The adoption of cloud data storage infrastructure provides enormous cost advantage to institutions handling big data to capture, process, share and access information quickly. However, this has equally exposed them to heightened security risks and unauthorized access to classified information by criminals who may be state or non-state actors and have greater opportunity to intercept or steal the institutional information and data for

[11] Dahlman, Carl, Sam Mealy, and Martin Wermelinger. "Harnessing the digital economy for developing countries." (2016).
[12] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International journal of critical infrastructure protection* 25 (2019): 36-49.
[13] Glikson, Ella, and Anita Williams Woolley. "Human trust in artificial intelligence: Review of empirical research." *Academy of Management Annals* 14, no. 2 (2020): 627-660.
[14] Shafqat, Narmeen, and Ashraf Masood. "Comparative analysis of various national cyber security strategies." *International Journal of Computer Science and Information Security* 14, no. 1 (2016): 129-136.

their own unlawful use. This study thus set to examine the information security threats to e-government services in Kenya as a modern developing state in a highly interconnected world with limited sovereign control and capabilities in the cyberspace.

## 1.3 Objectives of the Study

The general objective of the study was to examine the information security threats to e-government services in Kenya with the following specific objectives:

1. To examine the types of public services offered on e-government platforms in Kenya
2. To investigate the types of information security threats to e-government services in Kenya.
3. To identify the information security measures required to protect the e-government services in Kenya.

## 1.4 Research Questions

The study was guided by the following research questions derived from the specific objectives:

1. What are the types of public services provided by e-government services in Kenya?
2. What are the types of information security threats to e-government services in Kenya?
3. What types of information security measures are required to protect the e-government services in Kenya?

## 1.5 Hypothesis of the study

The study tested the following hypotheses:

### 1.5.1 Specific Objective 1: Type of Public Services

H0: The type of public services have no effect on the quality of e-government services in Kenya.

H1: The type of public services have significant effect on the quality e-government services in Kenya.

### 1.5.2 Specific Objective 2: Types of information security threats

H0: The types of information security threats have no effect on the quality on e-government services in Kenya.

H1: The types of information security threats have significant effect on the quality on e-government services in Kenya.

### 1.5.3 Specific Objective 3: Information Security Measures

H0: The types of information security measures have no effect on the quality of e-government services in Kenya.

H1: The types of information security measures have significant effect on the quality of e-government services in Kenya.

## 1.6 Scope of the study

The study examined the information security threats to the provision of e-government services in Kenya and was scoped with three study objectives i.e The Kenya government

public services offered through the e-government platforms, the information security threats and the preventive measures necessary to safeguard the operations of the e-government services. The study independent variable was the e-government services while the dependent variables were information security threats and security measures.

## 1.7 Justification of the Study

This study is important to the policymakers in Kenya, particularly to the Ministry of Information Communication and Technology (ICT) and key government departments to help improve policy practice for better management and protection of classified government information. The study will benefit other stakeholders dealing with the government to improve their operational procedures for efficient delivery and access to e-government services. The study will additionally benefit the academia with easy access to reference materials and clear understanding of the information security threats and challenges highlighted by the study and further provide rich data for future research.

## 1.8 Literature Review

The research study examined information from secondary sources and the listed concepts and scope was identified, summarized and analysed in the report as major literal studies within the stated study objectives as both empirical and theoretical reviews.

### 1.8.1 Theoretical Framework

The study was guided by Ludwig Von Bertalanffy, General System Theory (GST). This theory has inter-disciplinary application and adoption borrowing from biology, engineering, mathematics, sociology, philosophy, political science, organizational

studies, communications and information science.[15] The proponents of this theory observe that systems are unique and forms inter-dependent relationships among the components establishing patterns and structures in a hierarchical relationship and ordering.[16]

This study takes view that the modern communication is a conglomeration of sub-systems that are quite unique and interdependent among each other through a fusion of people, infrastructure, technology and information.[17] The research examined the potential security risks and threats to the e-government platform from within the approach of an independent system with potential interconnectivity or interdependence organized structurally and supporting each other within the networks.

### 1.8.2 Empirical Literature Review

The empirical review focused on the following major concepts and ideas within the information, communications, organizations, engineering, social sciences among many other disciplines on cross-cutting basis.

### 1.8.3 Globalisation

The concept of globalisation has been around for a few decades gaining popularity in the 20th Century. In the 21st Century, a number of scholars came up to elucidate differing debates on the concept for lack of acceptable common definition of globalisation. Some scholars observe that modernisation and technological transformations have made the

[15] Craig R. Scott and Laurie Lewis, The International Encyclopedia (2018), 106.
[16] Montuori, A. Systems Approach. *Encyclopedia of Creativity*, Academic Press ( 2011), Pp. 414–21
[17] Poole, M. S. Systems theory. ( CA: Sage , 2014), pp. 49–74.

world more connected and interdependent leading to improved movements, trade, commerce and communication. This has significantly reduced time and lowering associated costs.[18] Others argue that the physical geography of the world has never changed. The established international and national boundaries including populations continue to remain largely intact without any physical change. [19]

This study borrows from the schools of thought that identify globalisation as that process of increased interconnectivity and interdependence in the world systems made possible through technological advances in science, information, communication, and technology that have made it easy for the world to trade, move, interact and communicate easily impacting significantly on their political, economic, cultural and social activities.[20]

### 1.8.4 Science Technology and Innovations (STI)

The Science, Technology and Innovations (STI), has had magnificent impact on the world society. The major leading nations in science and technology have leaped into astronomical economic wealth and in the creation of high technology goods and services. They developed nations have registered big volumes of world commerce and trade. Their societies continue to enjoy high quality of life accessing superior goods and services comparatively. The Global Innovation Development Index (GIDI) rates above the industrialized world showing unequal imbalance between the North-South divide. The

[18] Wolf, M. Shaping Globalization. (Washington DC: IMF, 2014), 51. Accessed on 20 August 2022.
[19] Albrow et al, Globalization, Knowledge and Society. (London: Sage, 1990), pp.300-315.
[20] James, Paul and Steger, Manfred B. A Genealogy of globalization (Washington DC: Globalizations, 2014), pp. 417–34.

United States, Europe, and Eastern Asia lead the park in science and technology associated with big investments in Research and Development (R&D) programmes. [21]

### 1.8.5 Information Communication and Technology

Information and Communication Technology (ICT), sometimes referred to as Information Technology (IT) has been the main drive in collapsing global space and time enhancing a number of revolutions along the line.[22] The modern computing technologies, software, programming combined with communication advances such as mobile telephony, growth of internet communication technologies have been instrumental in most of the transformation witnessed in the sector. [23]

The society has transformed conduct of business and the locations nor do distances no longer matter as people are able to effectively and efficiently communicate, transact and interact widely from the palms of their hands without time limitations. These transformations have increased pressure on the state and business firms to adopt to new technology to keep pace with societal changes. These developments have given the modern state additional responsibility in the development of essential network infrastructure to support the provision of services. [24]

[21] Bergquist, K., Fink, C., & Raffo, J. Global Innovation Index , (Geneva: Cornell, 2018), WIPO. 193–209
[22] Martin Hilbert and Priscila López. The World's Technological Capacity to Store, Communicate, and Compute Information, Science, 2011, 332 (6025), pp. 60-65.
[23] Wells, G. Insight: The cybersecurity threats, ( London: Sage, 2019), 232
[24] Anderson, Monica. Mobile Technology, (2019), Pew Research Center, 5, pp.35-40.

### 1.8.6 E-Governance

E-Government refers to government agencies adaptation of science, communication and technology in the provision of public services to the citizens, businesses entities and outside organizations including foreigners and international agencies. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions. [25]

E-government initiatives are characterized by extensive use of web technologies which have transformed technology from pure information-sharing phase to interactive, transactional, and intelligent phases. Many states started making use of these technologies for web-based government services for improving government efficiency, transparency, and competitiveness in the global economy. Despite the increasing popularity and substantial growth in the development of e-government services on the internet, the e-government stumbles upon security and privacy threats. In general, the internet users have growing concerns of cyberspace identity thefts and privacy violations. The e-government sites become potential targets for cyber attackers and terrorists. Cyber intrusions into e-government network systems could harm e-government services any time if the e-government sites are not properly secured[26]. This study sought to examine information security threats to the e-government services in Kenya.

[25] Wells, G. Insight: The cybersecurity threats, ( London: Sage, 2019), 232
[26] Owigar, J. & Omwenga, E.I. User-centric evaluation, ( *International Journal of Computer Applications,2018),* 148 (8):17-23.

### 1.8.7 Information Security

This study focused on importance of information security to a state, organization or to the lowest level of an individual. There are many definitions of information Security popularly known as (infosec), for the purpose of this study, information security implies the mechanisms employed by governments, institutions and individuals to protect themselves against unauthorized or unintentional loss, destruction, access, denial or modification of information and data. Information is a major item of value for any organization fundamental to key decision making and must therefore be protected viciously. [27] Nations and Organizations employ various policy procedures and mechanisms for protecting their citizens, firms, employees, assets, critical infrastructure and data against unauthorized interference which may take many forms such as network security, infrastructure security, applications security, cyber security, cloud security among many other defence and protective measures[28] . It is important for the organizations to observe the information principles of confidentiality, integrity and accessibility for effective management and achievement of organizational information goals and objectives to meet the demands of their customers or clients. [29]

### 1.8.8 Gaps in the Literature

The theoretical and empirical literature reviews established that implementation of the e-government services in Kenya is still an ongoing project where over 42 Counties with a

---

[27] Chanchala, Joshi, and Singh, Umesh Kumar. *"Information security risks "*. Journal of Information Security and Applications. (June, 2017), 35: 128–137.

[28] Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." *Computers & security* 49 (2015): 70-94.

[29] Kremling, Janine., Amanda, M., Sharp Parker. Cyberspace, Cybersecurity and Cybercrime. (London: SAGE Publications, 2018). 110

total of 51 Huduma Centres have been established countrywide with another 5 Counties in the pipeline. The ones established provide limited services on pilot basis with over 3000 different services on offer projected to rise to over 5000 by 2030. The information security threat to the services have not been fully scoped and thus this study undertook this examination exercise to cover the target population.

## 1.9 Research Methodology

### 1.9.1 Research Design

The research design constitutes the blue print for the collection, measurement and analysis of data.[30] The study used a descriptive research design framework in the collection, analysis, presentation and analysis of data in response to the problem of the study. The mixed method cross sectional survey approach was further chosen. This allowed the collection of both qualitative and quantitative data during the months of October and November 2022. The study considered this objective, reliable and representative in enhancing validity and reliability of the study findings from the population drawn from Huduma Service Centres in Kenya. The study variables were; the government services, the information security threats, the consequences of information security threats and the preventive measures against information security threats to e-government services in Kenya. The study further issued a pilot survey that was used to pretest and correct the information used in the conduct of final field questionnaire.

[30] Kothari, C.R. (2005), *" Research Methodology: Methods and Techniques"* New Age PublishersMarsh.D. and & Stolker, G. ( 2010) Theory and Methods in Political Science. London: Palyave Macmillan.

### 1.9.2 Target Population

Target population in statistics is the specific population about which information is desired.[31] A population is a set of people, services, elements, events, group of things or households that are being investigated. This definition ensures that population of interest is homogeneous.[32] The population of this study were all potential users of Kenya government services from the 51 Huduma Centres targeting both Kenyans and foreigners. Individuals, companies and international agencies. The target population for this study were service providers and users who sought Kenya government services on Wednesday, 2 November 2022 from ten (10) service Centre/ categories purposively chosen across the country out of the existing 51 Centres in Kenya including foreign segment. The study would have benefited more by conducting a national survey to cover all service Centres which however could not be viable due to limited time, resources and complex nature of conducting such research beyond the capabilities of the researcher.

### 1.9.3 Study Sample and Sampling Techniques

The study adopted purposive simple random sampling techniques. This is a procedure of selecting a subject to be included for a study by allocating equal chances to the elements in the population. [33] Sampling frame was used by allocating numbers to potential respondents from the target population. The purposive sampling allowed the study to access respondents that had the required information with respect to the objectives of the

[31] Creswell, John W., and J. David Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017

[32] Creswell,W. J. (2007). Qualitative Inquiry and Research Design: Choosing Among Five Approaches, London: Sage Publications.

[33] Creswell,W. J. (2007). Qualitative Inquiry and Research Design: Choosing Among Five Approaches, London: Sage Publications.

study. [34] The research considered this approach because the sample population was easily accessible, informative and knowledgeable on government services and aspects of information security that relate to electronic governance. The sample must be as big enough to provide representative results of the population. The sample size of 10 % was considered sufficient and representative. [35] The study targeted 1200 respondents from a target population of 12000 people drawn by the sample frame from 9 regions in Kenya and 1 segment representing foreigners (Non-Kenyans) as tabulated under.

**Table 1.1 Target Population and Sampling**

| **Population Location** | **Population Description** | **Target Population** | **Sample Size (%)** | **Sample Size (Nos)** | **Cum (%)** |
|---|---|---|---|---|---|
| Embu Town | Service Providers/Users | 1000 | 10 | 100 | 10 |
| Foreigners | Service Users | 1000 | 10 | 100 | 20 |
| Garissa Town | Service Providers/Users | 1000 | 10 | 100 | 30 |
| Kakamega Town | Service Providers/Users | 1000 | 10 | 100 | 40 |
| Kisumu Town | Service Providers/Users | 1000 | 10 | 100 | 50 |
| Mombasa Town | Service Providers/Users | 1000 | 10 | 100 | 60 |
| Nyeri Town | Service Providers/Users | 1000 | 10 | 100 | 70 |
| Nairobi GPO | Service Providers/Users | 1000 | 10 | 100 | 80 |
| Nairobi, City Sq | Service Providers/Users | 1000 | 10 | 100 | 90 |
| Nakuru Town | Service Providers/Users | 3000 | 10 | 300 | 100 |
| **Totals** | | **12000** | | **1200** | |

[34] Creswell. J.W. and Creswell, J.D. (2017) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition, Sage, Newbury Park

[35] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.

### 1.9.4 Data Collection Instrument

The research study used structured questionnaires that were administered and filled by the respondents. The questionnaires had both closed and open ended questions for the respondents to record their answers. The instrument was used to collect primary quantitative data and found to be suitable for this study because the researcher had the potential to reach a big number of respondents in a short period of time, provide respondents with adequate time to respond, anonymous and objective since the instrument does not result in biases of personal characteristics.[36] The research questionnaire was organized in according to the major objectives of the study and comprised four sections covering demographic information, government services, information security threats and the preventive measures to safeguard information security threats against the e-governance platform.

### 1.9.5 Piloting

The researcher undertook a pilot study with a tenth of the sample population in the neighboring Kiambu County region with a sample that was considered homogeneous to the target population of the study. This was very important to test the validity of the data collection and measurement instrument to enable effective and efficient roll out of the field study. The pilot study was conducted after obtaining research authorization from the National Commission of Science, Technology and Innovation (NACOSTI) and the National Defence University –Kenya (NDU-K). The pilot study will gave the researcher

[36] Creswell, J. W. (2011). Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research (4th Ed). New Delhi: Pearson Education Inc.

the opportunity to improve the quality of the research instrument and correction of data collection errors.

### 1.9.6 Data Analysis and Presentations

The completed study questionnaires which were received back from the respondents were sorted and checked for errors, omissions and biases. The data was further classified, categorized using tables. The researcher used both quantitative and qualitative statistical analysis using the Statistical Package of Social Science (SPSS) data processing tool. The results were presented in tables, pie-charts, frequency and percentages. Content analysis was further used to process the qualitative data collected by the open ended questions which were converted into quantitative data through the ordinal scale for ease of analysis and interpretation. Analysis of Variance was used to test the level of significance of the variables on the dependent variable at 95% confidence level.[37]

### 1.9.7 Ethical Considerations

The study strictly adhered to research ethics and standards as outlined in the NACOSTI and the NDU-K research policy. The questionnaire was explicit and gave complete assurance of the respondents' confidentiality. Other than voluntary participation in the study, the questionnaires remained anonymous and the researcher upheld the highest integrity in the collection of the data and adhered to all the statutory requirements and policy guidelines.

### 1.9.8 Chapter Outline

Chapter 1

[37] Creswell, J. W., & Creswell, J. D. (2018). Research design (5th ed.). SAGE Publications.

This chapter is the introduction chapter that covers the research proposal which contains the introduction, background, problem statement, study objectives, research questions, hypotheses, literature review, justifications, research methodology and ethical considerations.

Chapter 2

Chapter two analyses the study objective 1. The chapter examines the public services offered by the Kenya Government on e-government digital platforms and infrastructure.

Chapter 3

Chapter three analyses study objective 2. This chapter investigates the information security threats to the Kenya government e-services provision.

Chapter 4

Chapter four analyses study objective 3. This chapter investigates safeguard measures against information security threats to e-government services in Kenya.

Chapter 5

Chapter five presents study summary findings, conclusion and recommendations.

# CHAPTER TWO: THE STUDY POPULATION

## 2.0 Introduction

This chapter presents data, analysis, findings and discussions on the information security threats to the e-government service in Kenya. The data was collected using

questionnaires consisting of both close and open ended questions. This data has been analyzed using Statistical Package for Social Sciences (SPSS). The research findings are presented in tables, figures, graphs and descriptive statistics.

## 2.1 Questionnaires

The target population of the study was 12000 people and through purpose sampling the study targeted a sample size of 10% of the population and a total of 1200 questionnaires were sent out to the potential respondents in the 10 regions identified by the study. 966 respondents filled and returned the questionnaires making a response rate of 80%. The research response rate of 50% is considered adequate, rate of 60% is considered good and any rate above 70% is considered excellent.[38] Other writers consider a response rate of 50% to be adequate for analysis and reporting; a rate of 60% as good and a response rate of 70% and above is excellent.[39] Based on the above assertions, the response rate of 80% returned by this study was thus excellent to make credible deductions from the data collected and analysed by the study.

**Table 2.1 Questionnaires Response Rate**

| | **Questionnaires Administered** | **Questionnaires filled & Returned** | **Percentage Response** |
|---|---|---|---|
| **Respondents** | 1200 | 966 | 80% |

[38] Kothari, C. R., & Garg, G. Research Methodology: Methods and Techniques. New Delhi: New Age International Publishers, (2014).

[39] Hira, Tahira K., and Olive M. Mugenda. "The relationships between self-worth and financial beliefs, behavior, and satisfaction." *Journal of family and consumer sciences* 91, no. 4 (1999): 76

## 2.2 Demographic Information

The study sought to establish the demographic information of the population. These are the characteristics which have both direct and indirect influence on the objectives of the study. The elements of measurement included gender, age, level of education, nationality and period of interaction or residence in Kenya.

### 2.2.1 Gender Distribution

On the gender distribution of the respondents the results were presented on figure 4.1

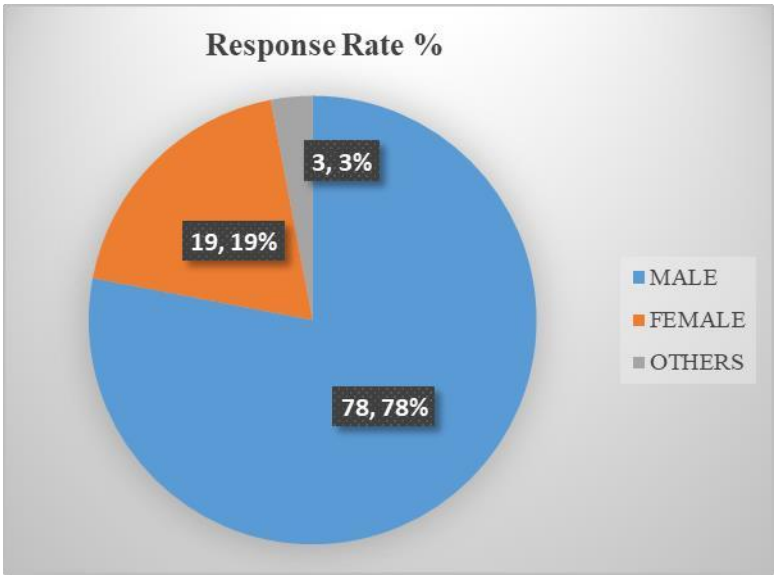


**Figure 2.1 Gender Distribution**

From the findings, 78.78% of respondents were males, 19.19% females and 3.3% from others. This shows that the study had more males than females. The reason for this was that males are more accessible than females due to the strong gender interaction culture. This representation is credible to allow assessment of the research objectives.

### 2.2.2 Age of Respondents

The findings on the age category are presented in the figure below.

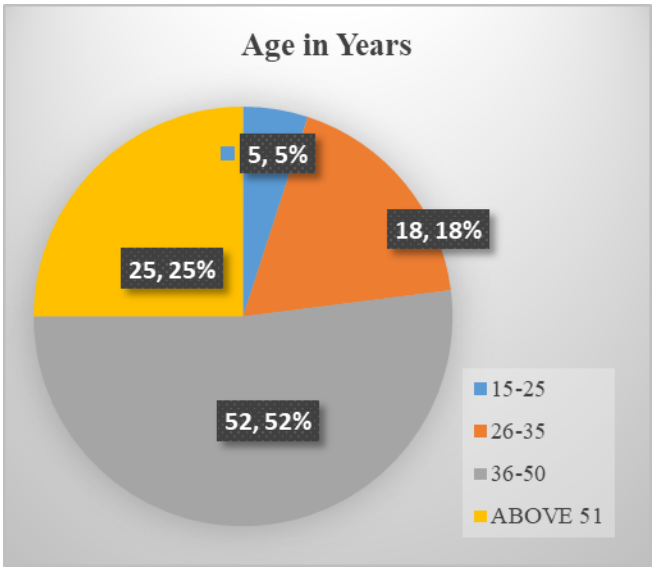


**Figure 2.2 Age of respondents in Years**

The respondents age distribution was analyzed as follows; Ages 15-25 years old 5.5%, ages 26-35 years old 18.18%, ages 36-50 years old 52.52% and ages 51 years and above 25.25%. This was a good indication that the respondents provided relevant information covered in the questionnaire. The older the responded the greater the experience and credible information provided pertaining to the research questions.

### 2.2.3 Level of Education

The findings on the distribution of the respondents in terms of Level of Education Attained were presented in the figure below.

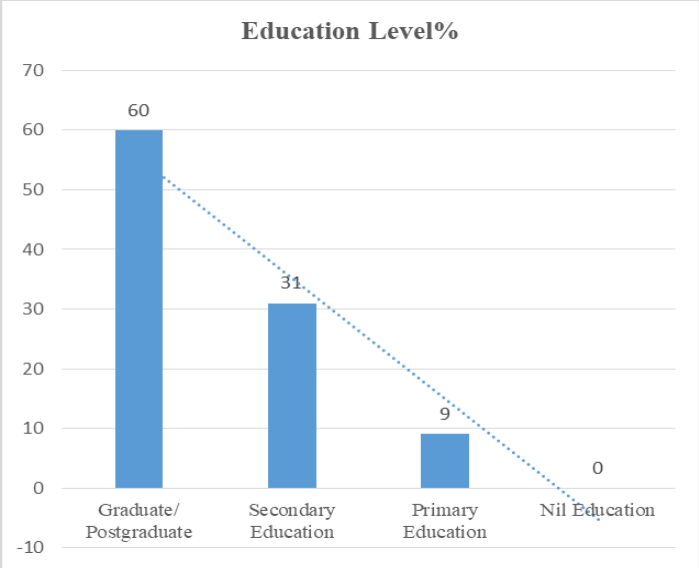


**Figure 2.3 Level of Education**

Based on this finding, the respondents had acquired formal education as follows; Primary Education 9%, Secondary Education 31%, Graduate Education 60% and Nil Education 0%. The study noted that majority had acquired formal education at a level of 90% which was excellent requirement for the research. The high literacy level is a positive indicator for the experience and knowledge in the subject matter of the study.

### 2.2.4 Nationality

The findings on respondents in terms of Nationality are presented in the figure below.

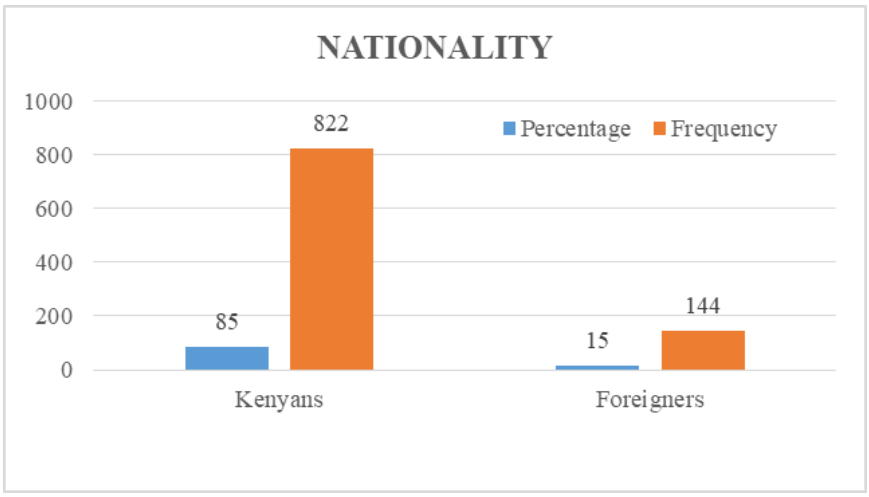


**Figure 2.4 Nationality**

Based on this findings, 822 respondents about 85% were Kenyans while 144 respondents about 15% were foreigners. The study thus managed to obtain data from both nationals and foreigners. This is important because government services are provided to both nationals and non-nationals. This gives the opportunity for the study to analyse good mix of the population of the study.

### 2.2.5 Period of Residence

The findings on the distribution of respondents in terms of residence in the region by the respondents were presented on the figure below.

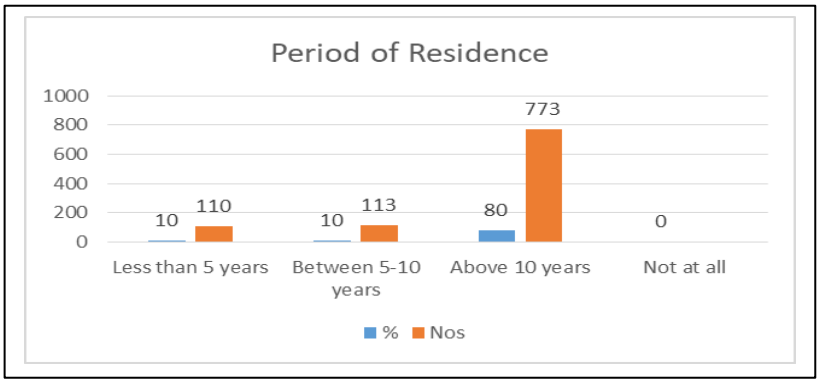

**Figure 2.5 Period of Residence**

The findings indicate that 80% of respondents have lived in Kenya for more than 10 years, 10% have been in Kenya for a period of between 5-10 years and another 10% have been in the country for less than 5 years. Period of residence by the respondent was of interest to the study because it correlates to the experience of respondents with the services offered by the Kenya government.

### 2.2.6 Category of Respondents

The findings from the respondents is presented in the figure below.

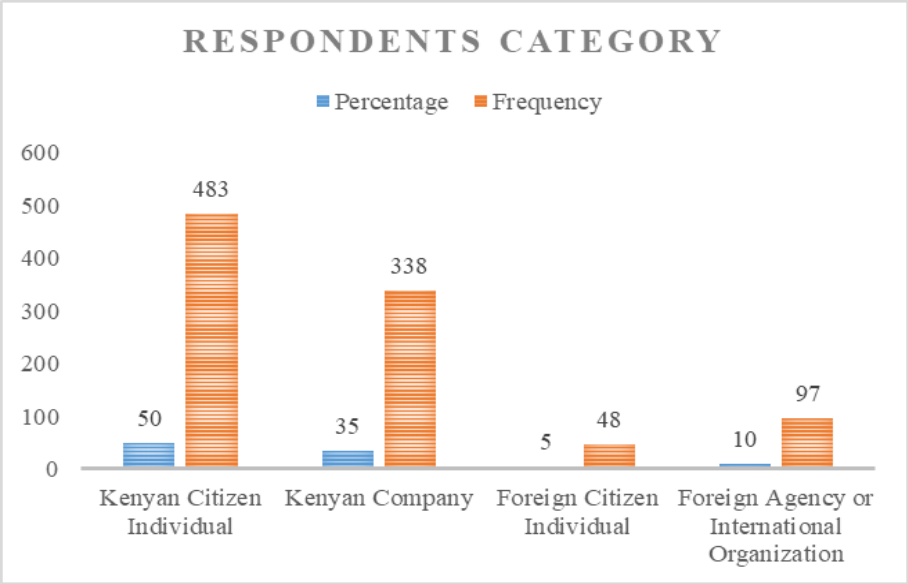


**Figure 2.6 Category of Respondents**

The study found that Kenyan citizens were the majority at 50%, followed by Kenyan registered Companies at 35%, then Foreign Citizen individuals at 5% and Foreign Agencies 10%. The category of the respondents was of interest to the study since this

would provide good indicator on their personal interaction and experience with the government services in Kenya.

### 2.2.7 Respondents Seeking Government Services

The findings from the respondents is presented in the figure below.

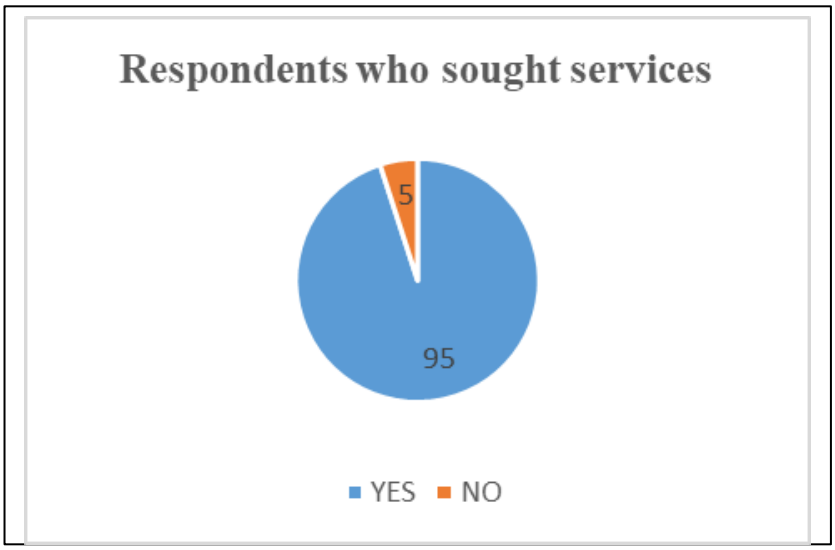


**Figure 2.7 Respondents who sought government services**

From the findings, 95% of respondents have sought for public services in Kenya while 5% had not. This is a positive indicator towards achievement of the objective of the study. The higher response level of 95% guarantees that the information sought from the elements of the population will have greater influence in response to the questions on challenges facing the provision of public services in Kenya. This representation is credible to allow effective assessment of the research objectives. The 95 % response rate of the sample is a positive indicator that can be inferred of the overall population of the study. This implies that the majority of the population have since embraced digital or online services being offered by the government of Kenya.

### 2.2.8 Categories of Government Services

The findings from the respondents are presented in the Tables below:

**Table 2.2 Categories of Government Services**

| Kenya Government Services | % | Freq | Cum % Freq |
|---|---|---|---|
| Government to Citizen (G2C) Civil Registrations, Property, general services(e-citizen, i-tax, nhif...) | 43 | 415 | 43 |
| Government to Business (G2B) Licences, Revenues, Taxations, Permits (e-citizen, i-tax, ifmis, erp, nhif... | 35 | 339 | 78 |
| Government to Government (G2G) Private and commercial services (e-commerce, i-tax, collaborations) | 2 | 19 | 80 |
| Government to Employees (G2E) Salaries, Reports, instructions, Returns (ifmis, erp...) | 20 | 193 | 100 |
| **Totals Respondents** | **100** | **966** | |

Based on these findings, 415 respondents representing 43% were citizens who sought government services (G2C), 339 respondents representing about 35% sought Government to Business (G2B) services, 19 respondents representing 2% sought Government to Government services and 193 respondents representing 20% sought Government to employees services. The study thus managed to obtain data from both nationals and foreigners. This is important because government services are provided to both nationals and non-nationals. This gives the opportunity for the study to analyse a good mix of the population of the study who sought government services by their categories. The descriptive analysis is further presented in the table below:

| Element | Value | |
|---|---|---|
| Mean | | 241.5 |
| Standard Error | | 87.30549811 |
| Median | | 266 |
| Mode | #N/A | |
| Standard Deviation | | 174.6109962 |
| Sample Variance | | 30489 |
| Kurtosis | | -1.118353169 |
| Skewness | | -0.623577748 |
| Range | | 396 |
| Minimum | | 19 |
| Maximum | | 415 |
| Sum | | 966 |
| Count | | 4 |
| Confidence Level(95.0%) | | 277.8450599 |

**Figure: 2.8 Government Public Services**

### 2.2.9 Methods of Government Services

The findings from the respondents is presented in the figure below.

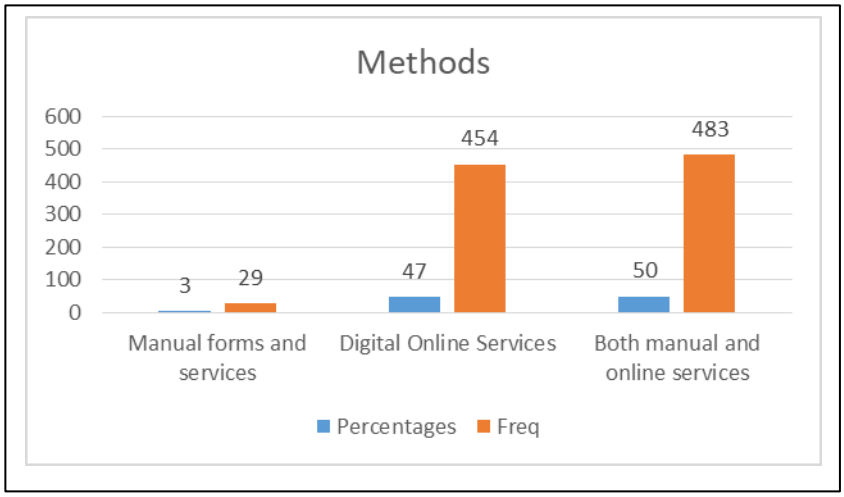


**Figure 2.9 Methods/Platform of services**

From the findings above, of the respondents who sought public services, only 3% obtained them through a manual system, 47% transacted through a digital/online platform and 50% obtained them through a mixed manual/digital interface. This is a positive indicator that the majority of respondents obtained public services through a digital platform. These responses indicate that the Kenya government has largely adopted digitization of services in areas with essential digital infrastructure supporting online services. This representation is credible to allow for the analysis of the research objectives.

### 2.2.10 Level of Services

The findings from the respondents is presented in the figure below.

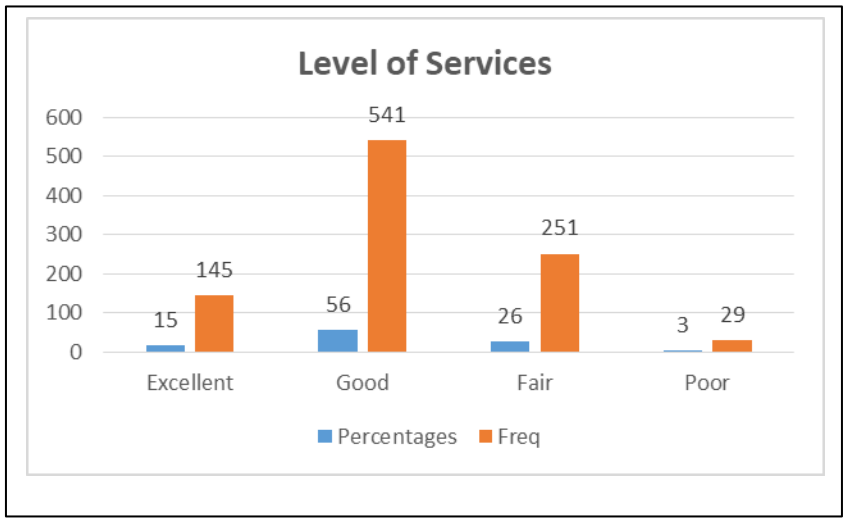


**Figure 2.10 Level of services**

From the findings above, 15% of respondents were extremely happy with the quality of public services, 56% rated the services as good, while 26% of the respondents rated the services as fair and 3% of the respondents rated the services as poor. This is a positive

indicator of public service delivery given the fact that over 71% of the respondents rated the quality of services above average. This representation is credible to allow for the effective analysis of the research objectives.

### 2.2.11 Hypothesis Testing

The specific objective was to examine types of public services offered and their effect on the quality of the e-government services. The following hypothesis was tested at significance level of 5% using the SPSS software:

**H0:** The type of public services have no effect on the quality e-government services in Kenya.

**H1:** The type of public services have significant effect on the quality e-government services in Kenya.

**$Chi^2$ –Test = $x^2$ , df 3 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 10.83**

The $Chi^2$ –Test of 10.83 is significantly greater than the critical value of 9.35 at 5% significant level. We thus reject the Null Hypothesis (H0) and accept the Alternative Hypothesis (H1) that the type of services have significant effect on the quality of e-government services.

### 2.2.12 Summary Findings

Findings from this chapter observes that 78.78% of respondents were males, 19.19% females and 3.3% from others, age distribution was analyzed as follows; Ages 15-25 years old 5.5%, ages 26-35 years old 18.18%, ages 36-50 years old 52.52% and ages 51 years and above 25.25%. Based on this finding, the respondents had acquired formal education as follows; Primary Education 9%, Secondary Education 31%, Graduate

Education 60% and Nil Education 0%. Based on this findings, 822 respondents about 85% were Kenyans while 144 respondents about 15% were foreigners. The findings further indicate that 80% of respondents have lived in Kenya for more than 10 years, 10% have been in Kenya for a period of between 5-10 years and another 10% have been in the country for less than 5 years.

The study found that Kenyan citizens were the majority at 50%, followed by Kenyan registered Companies at 35%, then Foreign Citizen individuals at 5% and Foreign Agencies 10%. From the findings, 95% of respondents have sought for public services in Kenya while 5% had not. Based on these findings, 415 respondents representing 43% were citizens who sought government services (G2C), 339 respondents representing about 35% sought Government to Business (G2B) services, 19 respondents representing 2% sought Government to Government services and 193 respondents representing 20% sought Government to employee services.

From the findings above, of the respondents who sought public services, only 3% obtained them through a manual system, 47% transacted through a digital/online platform and 50% obtained them through a mixed manual/digital interface. From the findings above, 15% of respondents were extremely happy with the quality of public services, 56% rated the services as good, while 26% of the respondents rated the services as fair and 3% of the respondents rated the services as poor. From the findings above, 15% of respondents were extremely happy with the quality of public services, 56% rated the services as good, while 26% of the respondents rated the services as fair and 3% of the respondents rated the services as poor. The **Chi$^2$ –Test** of 10.83 > 9.35 was significantly greater at 5% significant level rejecting the Null Hypothesis (H0). Thus the Alternative Hypothesis (H1) stating that the type of services have significant effect on the quality of e-government services was accepted.

## CHAPTER THREE: INFORMATION SERCURITY THREATS

### 3.0 Introduction

This chapter presents data, analysis, findings and discussions on objective two of the study. This objective identified the scope and extent of information security threats to the provision of e-government service in Kenya. The data was compiled from section two of the field questionnaires issued to the study respondents. The section comprised both close and open ended questions. This data has been analysed using Statistical Package for Social Sciences (SPSS). The research findings are thus presented in tables, figures, graphs and descriptive statistics.

### 3.1 Field Questionnaires issued and responses

**Table 3.1 Questionnaires Response Rate**

| | Questionnaires Administered | Questionnaires filled & Returned | Percentage Response |
|---|---|---|---|
| **Respondents** | 1200 | 966 | 80% |

The target population of the study was 12000 people and through purpose sampling the study targeted a sample size of 10% of the population and a total of 1200 questionnaires were sent out to the potential respondents in the 10 regions identified by the study. 966 respondents filled and returned the questionnaires making a response rate of 80%. The research response rate of 50% is considered adequate, rate of 60% is considered good and any rate above 70% is

considered excellent.[40] Other writers consider a response rate of 50% to be adequate for analysis and reporting; a rate of 60% as good and a response rate of 70% and above is excellent.[41] Based on the above assertions, the response rate of 80% returned by this study was thus excellent to make credible deductions from the data collected and analysed by the study.

## 3.2 Information Security Threats to E-government Services

**Table 3.2 Information Security Threats Respondents by Numbers**

| | Type of Security Threat | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree | Totals |
|---|---|---|---|---|---|---|---|
| 1. | Unauthorized access, interference and interference | 66 | 83 | 127 | 428 | 262 | 966 |
| 2. | Illegal devices | 76 | 107 | 156 | 378 | 249 | 966 |
| 3. | Unauthorized codes and passwords | 93 | 76 | 191 | 370 | 236 | 966 |
| 4. | False publications | 59 | 113 | 154 | 372 | 268 | 966 |
| 5. | Computer frauds and forgery | 81 | 58 | 85 | 335 | 407 | 966 |
| 6. | Cyber espionage terrorism and squatting | 66 | 66 | 160 | 342 | 332 | 966 |
| 7. | Phishing | 79 | 71 | 156 | 392 | 268 | 966 |
| 8. | Identity theft and impersonation | 66 | 66 | 122 | 372 | 340 | 966 |
| 9. | Interception of electronic messages and money transfer | 74 | 66 | 158 | 328 | 340 | 966 |
| 10. | Fraudulent use of electronic data | 71 | 66 | 97 | 392 | 340 | 966 |
| 11. | Employee irresponsibility, aiding or abetting offences | 97 | 70 | 119 | 356 | 324 | 966 |
| 12. | Child pornography | 151 | 111 | 214 | 267 | 223 | **966** |
| | **Sub Totals** | **979** | **953** | **1739** | **4332** | **3589** | |

[40] Kothari, C. R., & Garg, G. Research Methodology: Methods and Techniques. New Delhi: New Age International Publishers, (2014).

[41] Hira, Tahira K., and Olive M. Mugenda. "The relationships between self-worth and financial beliefs, behavior, and satisfaction." *Journal of family and consumer sciences* 91, no. 4 (1999): 76

This table is a summary of respondents who identified common information security threats to the provision of e-government services in Kenya. They identified 12 categories of threats tabulated above. 3589 responses strongly disagreed, 953 responses disagreed, 1739 responses neither agreed nor disagreed, 432 responses agreed and 3589 responses strongly agreed. The data indicates that 966 respondents returned 3671 negative responses at 32% and 7129 positive responses at 68%. This was relatively good response because any response above 60% is considered good for decision making.

**Table 3.3 Information Security Threats Respondents by Percentages (%)**

| | **INFORMATION SECURITY THREATS** | **Strongly Disagree** | **Disagree** | **Neutral** | **Agree** | **Strongly Agree** | **Totals** |
|---|---|---|---|---|---|---|---|
| 1 . | Unauthorized Access, Interferences | 6.83 | 8.59 | 13.15 | 44.31 | 27.12 | 100 |
| 2 . | Illegal Devices | 7.87 | 11.08 | 16.15 | 39.13 | 25.78 | 100 |
| 3 . | Unauthorized Codes and Passwords | 9.63 | 7.87 | 19.77 | 38.30 | 24.43 | 100 |
| 4 . | False Publications | 6.11 | 11.70 | 15.94 | 38.51 | 27.74 | 100 |
| 5 . | Computer Frauds and Forgery | 8.39 | 6.00 | 8.80 | 34.68 | 42.13 | 100 |
| 6 . | Cyber Espionage Terrorism and Squating | 6.83 | 6.83 | 16.56 | 35.40 | 34.37 | 100 |
| 7 . | Phishing | 8.18 | 7.35 | 16.15 | 40.58 | 27.74 | 100 |
| 8 . | Identity Theft and Impersonation | 6.83 | 6.83 | 12.63 | 38.51 | 35.20 | 100 |
| 9 . | Interception of Electronic Messages and Money Transfer | 7.66 | 6.83 | 16.36 | 33.95 | 35.20 | 100 |
| 10 . | Fraudulent use of Electronic Data | 7.35 | 6.83 | 10.04 | 40.58 | 35.20 | 100 |
| 11 . | Employee Irresponsibility, Aiding or Abetting Offences | 10.04 | 7.25 | 12.32 | 36.85 | 33.54 | 100 |
| 12 . | Child Pornography | 15.63 | 11.49 | 22.15 | 27.64 | 23.08 | |

The study sought to find the nature and types of information security threats that predisposes challenges and risks to the e-government services in Kenya from the study population. There exist in Kenya a number of legislative framework and regulations to protect Kenyans and official government information from the dangers of internet based cybercrimes.

The normative framework regulations includes; National ICT Survey Report (2010), Government of Kenya Cyber Security Strategy (2014), Kenya Information and Communications Amendment Bill (2019), The Kenya government Data Protection Act (2019), Digital Economy Powering Kenya's Transformation (2019), National Information and Communications Technology Policy 2019, Data Protection Act Civil registration Regulations (2020), National Elections Single Window systems Act 2022, Registrations of Person (NIIMS), Regulations 2020.

The sector has seen a number of the proliferation of legislations, policies and strategies all intended to protect Kenya and its citizens against the many internet based cybercrime threats and activities orchestrated by both individual criminals or state and non-state actors. The study originally identified twelve categories of information security threats that were subjected under investigation from the population. The study found out the following:

### 3.2.1 The unauthorized access and interference with system networks.

The study found that 6.83% Strongly Disagreed, 8.59% Disagreed, 13.15% Neither Agreed nor Disagreed, 44% Agreed and 27.12% Strongly Agreed. The study further made a finding that summative 28% largely disagreed and 72% equally agreed that unauthorized system access remained a significant security threat to government e-government services. According to Tahira and Mugenda, any findings above 70% is considered excellent.[42] Similar studies by Khisa, Odima and Wafula identified

[42] Hira, Tahira K., and Olive M. Mugenda. "The relationships between self-worth and financial beliefs, behavior, and satisfaction." *Journal of family and consumer sciences* 91, no. 4 (1999): 76

unauthorized network access and system interference as substantial threat to e-government services with the potential to cause data loss, system capture, phishing, data loss, alterations, disruptions and possible system destructions.[43]

### 3.2.2 Illegal Devices

The study found that 7.87% Strongly Disagreed, 11.08% Disagreed, 16.15% Neither Agreed nor Disagreed, 39.13% Agreed and 25.78% Strongly Agreed. The study further made a finding that summative 19% largely disagreed and 81% equally agreed that illegal devices remain a significant security threat to e-government services. According to Tahira and Mugenda, any findings above 70% is considered excellent.[44] The study thus deducts that illegal devices are potential security threat with the potential to cause system and service disruption and the organization must have a good policy procedure for handling and application of external inter-connected devices.

### 3.2.3 Unauthorized Codes and Password

The study found that 9.63% Strongly Disagreed, 7.87% Disagreed, 19.77% Neither Agreed nor Disagreed, 38.30% Agreed and 24.43% Strongly Agreed. The study further made a finding that summative 18% largely disagreed and 82% equally agreed that unauthorized codes and passwords remain a significant security threat to e-government services. According to Tahira and Mugenda, any findings above 70% is considered excellent. The study deducts that use of unauthorized codes and passwords are potential security threat which can cause system malfunction and services disruption.

---

[43] Khisa, M., Odima, Z., Wafula, R., Innovative Ways the Government of Kenya is Delivering Services to its Citizens through E-Government. School of Computing and Informatics, University of Nairobi 2020

[44] Hira, Tahira K., and Olive M. Mugenda. "The relationships between self-worth and financial beliefs, behavior, and satisfaction." *Journal of family and consumer sciences* 91, no. 4 (1999): 76

### 3.2.4 False Publications

The study found that 6.11% Strongly Disagreed, 11.70% Disagreed, 15.94% Neither Agreed nor Disagreed, 38.51% Agreed and 27.74% Strongly Agreed. The study further made a finding that summative 18% largely disagreed and 82% equally agreed that False Publications remain a significant security threat to e-government services. According to Tahira and Mugenda, any findings above 70% is considered excellent. The study deducts that false publications are potential security threats which can cause harm or mislead internet digital technology users because of disinformation and misinformation.

### 3.2.5 Computer Frauds and Forgery

The study found that 8.39% Strongly Disagreed, 6.0% Disagreed, 8.80% Neither Agreed nor Disagreed, 34.68% Agreed and 42.13% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that computer frauds and forgery remain a significant security threat to e-government services. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu , identified computer identity fraud as a major impediments to the e-governance systems and services.[45] The study deducts that use of unauthorized codes and passwords are potential security threat which can cause system malfunction and disruption services.

### 3.2.6 Cyber espionage, terrorism and squating

The study found that 6.83% Strongly Disagreed, 6.830% Disagreed, 16.56% Neither Agreed nor Disagreed, 35.40% Agreed and 34.37% Strongly Agreed. The study further

[45] Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage. Cyber Crime, Cyber Space and Effects of Cyber Crime. Volume 7, Issue 1 Page Number: 210-214 Publication Issue : January-February-2021

made a finding that summative 14% largely disagreed and 86% equally agreed that cyber espionage, terrorism and squatting were serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu , identified cyber espionage, terrorism and squatting as a major threats to the e-governance systems and services delivery.[46] The study deducts that cyber espionage, terrorism and squatting are potential security threat which can cause system malfunction, loss of data, loss of investment, disruption services and equipment loss or destruction.

### 3.2.7 Phishing

The study found that 8.18% Strongly Disagreed, 7.35% Disagreed, 16.15% Neither Agreed nor Disagreed, 40.58% Agreed and 27.74% Strongly Agreed. The study further made a finding that summative 15% largely disagreed and 85% equally agreed that phishing was a serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu , identified phishing as a major threats to the e-governance systems and services delivery. The study deducts that phishing is potential security threat which can cause system malfunction, loss of data, loss of investment, disruption services and equipment loss or destruction.

### 3.2.8 Identity theft and impersonation

The study found that 6.83% Strongly Disagreed, 6.83% Disagreed, 12.63% Neither Agreed nor Disagreed, 38.51% Agreed and 35.20% Strongly Agreed. The study further

[46] Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage. Cyber Crime, Cyber Space and Effects of Cyber Crime. Volume 7, Issue 1 Page Number: 210-214 Publication Issue : January-February-2021

made a finding that summative 14% largely disagreed and 86% equally agreed that identity theft and impersonation was a serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu, identified identity theft and impersonation as a major threats to the e-governance systems and services delivery. The study deducts that identity theft and impersonation was a potential security threat which can cause system malfunction, loss of data, loss of investment, disruption services and equipment loss or destruction.

### 3.2.9 Interception of electronic messages and money transfer

The study found that 7.66% Strongly Disagreed, 6.83% Disagreed, 16.36% Neither Agreed nor Disagreed, 33.95% Agreed and 35.20% Strongly Agreed. The study further made a finding that summative 15% largely disagreed and 85% equally agreed that interception of electronic messages and money transfer was a serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Khisa, Odima and Wafula, identified interception of electronic messages and money transfer as a major threats to the e-governance systems and services delivery.[47] The study deducts that interception of electronic messages and money transfer are potential security threats which can cause system malfunction, loss of data, loss of investment, disruption services and equipment loss or destruction.

[47] Khisa, M., Odima, Z., Wafula, R., Innovative Ways the Government of Kenya is Delivering Services to its Citizens through E-Government. School of Computing and Informatics, University of Nairobi 2020

### 3.2.10 Fraudulent use of electronic data

The study found that 7.35% Strongly Disagreed, 6.83% Disagreed, 10.04% Neither Agreed nor Disagreed, 40.58% Agreed and 35.20% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that fraudulent use of electronic data was a serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Khisa, Odima and Wafula, identified fraudulent use of electronic data as a major threats to the e-governance systems and services delivery.[48] The study deducts that fraudulent use of electronic data is potential security threat which can cause system malfunction, loss of data, loss of investment, disruption services and equipment loss or destruction.

### 3.2.11 Employee irresponsibility, aiding and abetting offences

The study found that 10.04% Strongly Disagreed, 7.25% Disagreed, 12.32% Neither Agreed nor Disagreed, 36.85% Agreed and 33.54% Strongly Agreed. The study further made a finding that summative 17% largely disagreed and 83% equally agreed that employee irresponsibility, aiding and abetting offences is serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Valentina Ndou, identified human capital development, essential skills and policy gap as a major threats to the effective implementation of n e-governance systems and services delivery.[49] The study

[48] Khisa, M., Odima, Z., Wafula, R., Innovative Ways the Government of Kenya is Delivering Services to its Citizens through E-Government. School of Computing and Informatics, University of Nairobi 2020
[49] Valentina (Dardha) Ndou. E – government for developing countries: opportunities and challenges. Ejisdc (2004) 18, 1, 1-24. Http://www.ejisdc.org

deducts that employee irresponsibility, aiding and abetting offences are potential security threat which can cause system malfunction, loss of data, loss of investment, disruption services and equipment loss or destruction.

### 3.2.12 Child Pornography

The study found that 15.63% Strongly Disagreed, 11.49% Disagreed, 22.15% Neither Agreed nor Disagreed, 27.64% Agreed and 23.08% Strongly Agreed. The study further made a finding that summative 27% largely disagreed and 73% equally agreed that child pornography is serious security threat to e-government platforms and services delivery. According to Tahira and Mugenda, any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu, identified child pornography as a major threats to the effective implementation of e-governance systems and services delivery.[50] The study deducts that child pornography has a potential security threat which can cause harm or mislead internet digital technology users particularly the young with fragile mindset because of disinformation and misinformation.

### 3.2.13 Other security threats

The study sought to gather other categories of information security threats that had been encountered by the study participants that had not been exclusively been covered by the questionnaires. The following is the summary extract of significant threats as identified by the respondents that have the potential to cause disruption of e-government services:

[50] Valentina (Dardha) Ndou. E – government for developing countries: opportunities and challenges. Ejisdc (2004) 18, 1, 1-24. Http://www.ejisdc.org

**Table 3.4 Other types of information security threats**

| | | Frequency | cum% |
|---|---|---|---|
| 1 . | Hacking | 20 | 20.00 |
| 2 . | Information Extortion | 10 | 30.00 |
| 3 . | Employee Mistakes | 5 | 35.00 |
| 4 . | Photoshop | 5 | 40.00 |
| 5 . | Corruption | 15 | 55.00 |
| 6 . | Service Providers | 20 | 75.00 |
| 7 . | Pharming, viruses, worms, access denial, bots | 15 | 90.00 |
| 8 . | Snooping | 10 | 100.00 |
| | **Totals** | 100 | |

### 3.2.14 Hypothesis Test

The specific objective was to investigate the types of insecurity threats that affect the quality of the e-government services. The following hypothesis was tested at a significance level of 5% (0.05) using the SPSS software:

**H0:** The information security threats have no effect on the quality of e-government services in Kenya.

**H1:** The information security threats have significant effect on the quality of e-government services in Kenya

**$Chi^2$ –Test = $x^2$ , df 11(n-1) = $\sum (Oi - Ei)^2 / Ei$ = 20.47**

The $Chi^2$ –Test of 20.47 is significantly greater than the critical value of 19.68 at 5% significant level. We thus reject the Null Hypothesis (H0) and accept the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya.

### 3.2.15 Chapter Summary

The summary findings from this chapter indicates that 966 respondents returned 3671 negative responses at 32% and 7129 positive responses at 68%. This was relatively good response because any response above 60% is considered good for decision making. The study further found that 6.83% Strongly Disagreed, 8.59% Disagreed, 13.15% Neither Agreed nor Disagreed, 44% Agreed and 27.12% Strongly Agreed. The study further made a finding that summative 28% largely disagreed and 72% equally agreed that unauthorized system access remained a significant security threat to government e-government services.

The study found that 7.87% Strongly Disagreed, 11.08% Disagreed, 16.15% Neither Agreed nor Disagreed, 39.13% Agreed and 25.78% Strongly Agreed. The study further made a finding that summative 19% largely disagreed and 81% equally agreed that illegal devices remain a significant security threat to e-government services. The study further found that 9.63% Strongly Disagreed, 7.87% Disagreed, 19.77% Neither Agreed nor Disagreed, 38.30% Agreed and 24.43% Strongly Agreed. The study further made a finding that summative 18% largely disagreed and 82% equally agreed that unauthorized codes and passwords remain a significant security threat to e-government services.

The study found that 6.11% Strongly Disagreed, 11.70% Disagreed, 15.94% Neither Agreed nor Disagreed, 38.51% Agreed and 27.74% Strongly Agreed. The study further made a finding that summative 18% largely disagreed and 82% equally agreed that False Publications remain a significant security threat to e-government services. The study

found that 8.39% Strongly Disagreed, 6.0% Disagreed, 8.80% Neither Agreed nor Disagreed, 34.68% Agreed and 42.13% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that computer frauds and forgery remain a significant security threat to e-government services.

The study found that 6.83% Strongly Disagreed, 6.830% Disagreed, 16.56% Neither Agreed nor Disagreed, 35.40% Agreed and 34.37% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that cyber espionage, terrorism and squatting were serious security threat to e-government platforms and services delivery. The study found that 8.18% Strongly Disagreed, 7.35% Disagreed, 16.15% Neither Agreed nor Disagreed, 40.58% Agreed and 27.74% Strongly Agreed. The study further made a finding that summative 15% largely disagreed and 85% equally agreed that phishing was a serious security threat to e-government platforms and services delivery. The study found that 6.83% Strongly Disagreed, 6.83% Disagreed, 12.63% Neither Agreed nor Disagreed, 38.51% Agreed and 35.20% Strongly Agreed.

The study further made a finding that summative 14% largely disagreed and 86% equally agreed that identity theft and impersonation was a serious security threat to e-government platforms and services delivery. The study found that 7.66% Strongly Disagreed, 6.83% Disagreed, 16.36% Neither Agreed nor Disagreed, 33.95% Agreed and 35.20% Strongly Agreed. The study further made a finding that summative 15% largely disagreed and 85% equally agreed that interception of electronic messages and money transfer was a serious security threat to e-government platforms and services delivery. The study found that

7.35% Strongly Disagreed, 6.83% Disagreed, 10.04% Neither Agreed nor Disagreed, 40.58% Agreed and 35.20% Strongly Agreed.

The study further made a finding that summative 14% largely disagreed and 86% equally agreed that fraudulent use of electronic data was a serious security threat to e-government platforms and services delivery. The study found that 10.04% Strongly Disagreed, 7.25% Disagreed, 12.32% Neither Agreed nor Disagreed, 36.85% Agreed and 33.54% Strongly Agreed. The study further made a finding that summative 17% largely disagreed and 83% equally agreed that employee irresponsibility, aiding and abetting offences is serious security threat to e-government platforms and services delivery. The study found that 15.63% Strongly Disagreed, 11.49% Disagreed, 22.15% Neither Agreed nor Disagreed, 27.64% Agreed and 23.08% Strongly Agreed.

Finally the study further made a finding that summative 27% largely disagreed and 73% equally agreed that child pornography is serious security threat to e-government platforms and services delivery. The study found that 15.63% Strongly Disagreed, 11.49% Disagreed, 22.15% Neither Agreed nor Disagreed, 27.64% Agreed and 23.08% Strongly Agreed. The study further made a finding that summative 27% largely disagreed and 73% equally agreed that child pornography is serious security threat to e-government platforms and services delivery. The **$Chi^2$ –Test** of 20.47 > 19.68 was significantly greater at 5% significant level rejecting the Null Hypothesis (H0). Thus the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya was accepted.

# CHAPTER FOUR: PREVENTIVE MEASURES

## 4.0 Introduction

This chapter presents data, analysis, findings and discussions on objective three of the study. This objective identified the preventive measures against information security threats to the provision of e-government service in Kenya. The data was compiled from section three of the field questionnaires issued to the respondents. The section comprised both close and open ended questions. This data has been analysed using Statistical Package for Social Sciences (SPSS). The research findings are thus presented in tables, figures, graphs and descriptive statistics.

## 4.1 Field Questionnaires issued and responses

**Table 4.1 Questionnaires Response Rate**

| | Questionnaires Administered | Questionnaires filled & Returned | Percentage Response |
|---|---|---|---|
| **Respondents** | 1200 | 966 | 80% |

The target population of the study was 12000 people and through purpose sampling the study targeted a sample size of 10% of the population and a total of 1200 questionnaires were sent out to the potential respondents in the 10 regions identified by the study. 966 respondents filled and returned the questionnaires making a response rate of 80%. The research response rate of 50% is considered adequate, rate of 60% is considered good and

any rate above 70% is considered excellent.[51] Other writers consider a response rate of 50% to be adequate for analysis and reporting; a rate of 60% as good and a response rate of 70% and above is excellent.[52] Based on the above assertions, the response rate of 80% returned by this study was thus excellent to make credible deductions from the data collected and analysed by the study.

## 4.2 Preventive Measures Against Information Security Threats

**Table 4.2 Preventive Measures by Respondents in Numbers**

| | **Preventive measures to information security threats** | **Strongly Disagree** | **Disagree** | **Neither Agree nor Disagree** | **Agree** | **Strongly agree** | **Totals** |
|---|---|---|---|---|---|---|---|
| 1 . | National legislations on information security is required | 62 | 31 | 71 | 337 | 465 | 966 |
| 2 . | Implement institutional policies, plans and strategies | 57 | 18 | 75 | 309 | 507 | 966 |
| 3 . | ICT training for service providers, vendors, operators and users is important | 53 | 44 | 84 | 238 | 547 | 966 |
| 4 . | Install end to end and back up computer security | 49 | 13 | 89 | 242 | 572 | 966 |
| 5 . | Enforce physical security, passwords and codes security control protocols for all users | 62 | 35 | 62 | 279 | 527 | 966 |
| 6 . | Employment and utilization of professional staff with appropriate certifications | 45 | 40 | 147 | 312 | 423 | 966 |
| 7 . | Frequent audits of ICT infrastructure, systems, programmes, procedures and regulations | 61 | 9 | 92 | 250 | 553 | 966 |
| 8 . | Install ICT hardware and software backups solutions and power systems | 53 | 18 | 107 | 254 | 534 | 966 |
| 9 . | Install computer and information security firewall and surveillance monitoring | 53 | 31 | 71 | 245 | | 966 |
| 10 . | Top management information security reviews | 54 | 23 | 108 | 266 | 515 | 966 |
| | **Sub Totals** | **551** | **262** | **907** | **2731** | **5210** | **9660** |

[51] Kothari, C. R., & Garg, G. Research Methodology: Methods and Techniques. New Delhi: New Age International Publishers, (2014).

[52] Hira, Tahira K., and Olive M. Mugenda. "The relationships between self-worth and financial beliefs, behavior, and satisfaction." *Journal of family and consumer sciences* 91, no. 4 (1999): 76

This table presents the summary of respondents who identified preventive measures against information security threats to the provision of e-government services in Kenya. The measures were grouped in 10 categories of threats tabulated above. 551 respondents strongly disagreed, 262 respondents disagreed, 907 respondents neither agreed nor disagreed, 2731 respondents agreed and 5210 respondents strongly agreed. The data results strongly indicates that 1719 respondents returned negative responses at 9% and 7941 respondents returned positive response at 91%. This was an excellent response because any response above 70% is considered extremely good and excellent for decision making.[53]

**Table 4.3 Preventive Measures against Information Security Threats Respondents by Percentages**

| | **Preventive measures to information security threats in %** | **Strongly Disagree** | **Disagree** | **Neutral** | **Agree** | **Strongly Agree** | **Totals** |
|---|---|---|---|---|---|---|---|
| 1 | National legislations on information security is required | 6 | 3 | 7 | 35 | 48 | 100 |
| 2 | Implement institutional policies, plans and strategies | 6 | 2 | 8 | 32 | 53 | 100 |
| 3 | ICT training for service providers, vendors, operators and users is important | 5 | 5 | 9 | 25 | 57 | 100 |
| 4 | Install end to end and back up computer security | 5 | 1 | 9 | 25 | 59 | 100 |
| 5 | Enforce physical security, passwords and codes security control protocols for all users | 6 | 4 | 6 | 29 | 55 | 100 |
| 6 | Employment and utilization of professional staff with appropriate certifications | 5 | 4 | 15 | 32 | 44 | 100 |
| 7 | Frequent audits of ICT infrastructure, systems, programmes, procedures and regulations | 6 | 1 | 10 | 26 | 57 | 100 |
| 8 | Install ICT hardware and software backups solutions and power systems | 6 | 2 | 11 | 26 | 55 | 100 |

[53] Kothari, C. R., & Garg, G. Research Methodology: Methods and Techniques. New Delhi: New Age International Publishers, (2014).

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9 | Install computer and information security firewall and surveillance monitoring | 6 | 3 | 7 | 25 | 59 | 100 |
| 10 | Top management information security reviews | 6 | 2 | 11 | 28 | 53 | 100 |

The study originally identified the above ten categories of preventive measures against information security threats to e-government services whose findings are further discussed under:

### 4.2.1 National Legislations

The study found that 6% of the respondents Strongly Disagreed, 3% Disagreed, 7% Neither Agreed nor Disagreed, 35% Agreed and 48% Strongly Agreed. The study further made a finding that summative 13% disagreed while 87% largely agreed that national legislations is a pre-requite for establishing protective framework against the information security threats that face the e-government services delivery in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[54] Similar study by Sunil, Pawar and Bapu, identified legislation, policies, rules, regulations and institutional procedures and processes as extremely important towards enhancing system operations and safety against information security violations.[55] The study thus deducts that national legislations, policies, rules and institutional regulations including protocols are necessary and important towards enhancing and protecting system confidentiality, integrity, information safety, operational efficiency and liabilities from third party stakeholders.

[54] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[55] Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage. Cyber Crime, Cyber Space and Effects of Cyber Crime. Volume 7, Issue 1 Page Number: 210-214 Publication Issue : January-February-2021

### 4.2.2 Institutional policies, plans and strategies

The study found that 6% of the respondents Strongly Disagreed, 2% Disagreed, 8% Neither Agreed nor Disagreed, 32% Agreed and 53% Strongly Agreed. The study further made a finding that summative 16% disagreed while 84% largely agreed that policies, plans and strategies are important institutional framework essential to guarantee protection against the information security threats that face the e-government services delivery in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[56] Similar study by Sunil, Pawar and Bapu, identified policies, rules, regulations extremely important towards enhancing system operations and safety against information security violations.[57] Amorreti identifies that for an effective e-democracy and e-governance system, the policies and regulations are essential not only to protect the system infrastructures and operators but equally important to focus the leadership vision and enhanced participation and decision making processes within the ICT ecosystem in the organization.[58] The study thus deducts that institutional policies, regulations and procedures are important in protecting system confidentiality, integrity, information safety, operational efficiency and third party liabilities against the organization.

### 4.2.3 ICT Training

The study found that 5% of the respondents Strongly Disagreed, 5% Disagreed, 9% Neither Agreed nor Disagreed, 25% Agreed and 56 % Strongly Agreed. The study further

[56] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[57] Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage. Cyber Crime, Cyber Space and Effects of Cyber Crime. Volume 7, Issue 1 Page Number: 210-214 Publication Issue : January-February-2021
[58] Amoretti, Francesco. "International organizations ICTs policies: e-democracy and e-government for political development." *Review of policy research* 24, no. 4 (2007): 331-344.

made a finding that summative 19% disagreed while 81% largely agreed that ICT training for the institutional operators, vendors and service providers was important institutional capacity building to guarantee protection against the information security threats that face the e-government services delivery in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[59] Irani et al observes that ICT skills are critical to bridge the digital divide in developing countries. Digital skills are essential for the design, implementation and management of the e-government platform and services. Development of relevant human capacities will facilitate effective management of the online services and maintenance of the systems, hence mandatory. [60] Similar study by Sunil, Pawar and Bapu, identified personnel training as not only essential but very important towards the protect the system infrastructures and customers data and privacy.[61] The study thus deducts that institutional capacity building through training is critical in protecting system confidentiality, integrity, information safety, operational efficiency and against third party liabilities against the organization.

### 4.2.4 Installation of end to end back up security

The study found that 5% of the respondents Strongly Disagreed, 1% Disagreed, 9% Neither Agreed nor Disagreed, 25% Agreed and 60% Strongly Agreed. The study further made a finding that summative 15% disagreed while 85% largely agreed that installation of end to end back up security was important institutional procedural undertaking and capacity building to guarantee protection against the information security threats that face

[59] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[60] Irani, Zahir, Peter ED Love, and Ali Montazemi. "E-government: past, present and future." *European Journal of Information Systems* 16, no. 2 (2007): 103-105.
[61] Amoretti, Francesco. "International organizations ICTs policies: e-democracy and e-government for political development." *Review of policy research* 24, no. 4 (2007): 331-344.

the e-government services delivery in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[62] Bacon et all observes that installation of end to end back up security as not only essential but very important towards the protection the system infrastructures and customers data and privacy.[63] The study thus deducts that installation of end to end back up security is critical in the overall protection of the system stability, integrity, information safety, operational efficiency, consistency, reliability and against third party liabilities.

### 4.2.5 Physical security, codes, passwords and control protocols

The study found that 6% of the respondents Strongly Disagreed, 4% Disagreed, 6% Neither Agreed nor Disagreed, 25% Agreed and 55% Strongly Agreed. The study further made a finding that summative 20% disagreed while 80% largely agreed that physical security, use of codes, authentic passwords and user procedures and protocols was important to guarantee protection against the information security threats that face the e-government services in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[64]

Camastra et al observes that installation of end to end back up security accompanied by physical equipment security, use of codes, authentic passwords and user protocols are not only essential but very important towards the protection the system infrastructures and

[62] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[63] Amoretti, Francesco. "International organizations ICTs policies: e-democracy and e-government for political development." *Review of policy research* 24, no. 4 (2007): 331-344.
[64] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.

equipment integrity.[65] The study thus deducts that physical security, use of codes, authentic passwords and user protocols are critical in the overall protection of the institutional ICT system infrastructure, stability, integrity, information safety, operational efficiency, consistency, reliability and against third party intrusions.

### 4.2.6 Employment of professionally certified staff

The study found that 5% of the respondents Strongly Disagreed, 4% Disagreed, 15% Neither Agreed nor Disagreed, 32% Agreed and 44% Strongly Agreed. The study further made a finding that summative 24% disagreed while 76% largely agreed that employment of professionally certified staff in the ICT function is a critical requirement to guarantee protection against the information security threats that face the e-government services. According to Tahira and Mugenda, any findings above 70% is considered excellent.[66] Lopez Vladimir observes that ICT skills are critical to bridge the digital divide in developing countries. Digital skills are essential for the design, implementation and management of the e-government platform and services.

Development of relevant human capacities will facilitate effective management of the online services and maintenance of the systems, hence mandatory. This requires the engagement, recruitment and mentoring of ICT professionally certified employees. [67] The study thus deducts that employment of professionally certified employees is very

[65] Camastra, Francesco, Angelo Ciaramella, and Antonino Staiano. "Machine learning and soft computing for ICT security: an overview of current trends." *Journal of Ambient Intelligence and Humanized Computing* 4 (2013): 235-247.
[66] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[67] López-Bassols, Vladimir. "ICT skills and employment." (2002).

important towards efficient, effective and protective delivery of ICT services and credible defence against the violation of the system integrity by information security threats.

### 4.2.7 Frequent audits of ICT infrastructures, systems, regulations and procedures

The study found that 6% of the respondents Strongly Disagreed, 1% Disagreed, 10% Neither Agreed nor Disagreed, 25% Agreed and 55% Strongly Agreed. The study further made a finding that summative 20% disagreed while 80% largely agreed that frequent audits of ICT systems, infrastructure and procedures is an important function to guarantee the institutional protection against the information security threats that face e-government services in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[68] According to Bambal et al, it is very important to undertake audit of the entire system infrastructure and procedures once implemented to determine the efficiency levels and effectiveness of the investment. He further observes five important dimensions of the e-government functions whose audit remains important to include, policy, institution, infrastructures, applications and planning.[69] The study thus deducts that frequent system, policy, infrastructure and procedures audits and integrity checks are critical in the overall protection of the institutional ICT infrastructure, stability, integrity, information safety, operational efficiency, consistency, reliability and against third party intrusions.[70]

---

[68] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.

[69] Sutopo, Bambang, Trisninik Ratih Wulandari, Arum Kusumaningdyah Adiati, and Dany Adi Saputra. "E-government, audit opinion, and performance of local government administration in Indonesia." *Australasian Accounting, Business and Finance Journal* 11, no. 4 (2017): 6-22.

[70] Gheorghe, Mirela. "Audit Methodology for IT Governance." *Informatica Economica* 14, no. 1 (2010).

### 4.3.8 Installations of hardware and software backups

The study found that 6% of the respondents Strongly Disagreed, 2% Disagreed, 11% Neither Agreed nor Disagreed, 26% Agreed and 55% Strongly Agreed. The study further made a finding that summative 19% disagreed while 81% largely agreed that installations of hardware and system software back ups are important protection and safeguards against the information security threats that face e-government services in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[71]

According to Bambal et al, it is very important for the organizations with heavy investments in ICT digital systems and infrastructure to install operational back up support for essential hardware and software applications.[72] The study thus deducts that installations of systems hardware and software backups are critical in the overall protection of the institutional ICT infrastructure, stability, integrity, information safety, operational efficiency, consistency, reliability and against third party intrusions.[73]

### 4.3.9 Installations of system security firewalls and automated monitoring

The study found that 6% of the respondents Strongly Disagreed, 3% Disagreed, 7% Neither Agreed nor Disagreed, 25% Agreed and 59% Strongly Agreed. The study further made a finding that summative 16% disagreed while 84% largely agreed that installations of system security firewalls and automated monitoring intelligence are important

[71] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[72] Sutopo, Bambang, Trisninik Ratih Wulandari, Arum Kusumaningdyah Adiati, and Dany Adi Saputra. "E-government, audit opinion, and performance of local government administration in Indonesia." *Australasian Accounting, Business and Finance Journal* 11, no. 4 (2017): 6-22.
[73] Gheorghe, Mirela. "Audit Methodology for IT Governance." *Informatica Economica* 14, no. 1 (2010).

protection and safeguards against the information security threats that face e-government services in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[74]

According to Mirella, it is important for the organizations with investments in ICT digital systems and infrastructure to install system firewalls and automated monitoring intelligence applications for sustained protection and redundancy of the digital investment.[75] The study thus deducts that installations of systems firewalls and automated surveillance are critical in the overall protection of the institutional ICT infrastructure, stability, integrity, information safety, operational efficiency, consistency, reliability and against third party intrusions.[76] The study found that 5% of the respondents Strongly Disagreed, 4% Disagreed, 15% Neither Agreed nor Disagreed, 32% Agreed and 44% Strongly Agreed. The study further made a finding that summative 24% disagreed while 76% largely agreed that employment of professionally certified staff in the ICT function is a critical requirement to guarantee protection against the information security threats that face the e-government services

### 4.3.10 Top Management Information Security Reviews

The study found that 6% of the respondents Strongly Disagreed, 2% Disagreed, 11% Neither Agreed nor Disagreed, 28% Agreed and 53% Strongly Agreed. The study further made a finding that summative 19% disagreed while 81% largely agreed that top

[74] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.
[75] Sutopo, Bambang, Trisninik Ratih Wulandari, Arum Kusumaningdyah Adiati, and Dany Adi Saputra. "E-government, audit opinion, and performance of local government administration in Indonesia." *Australasian Accounting, Business and Finance Journal* 11, no. 4 (2017): 6-22.
[76] Gheorghe, Mirela. "Audit Methodology for IT Governance." *Informatica Economica* 14, no. 1 (2010).

management information security reviews are important protection and safeguards against the information security threats that face e-government services in Kenya. According to Tahira and Mugenda, any findings above 70% is considered excellent.[77]

The management have the overall responsibility and accountable for the system efficiency and functionality in delivery of services to the public. As the policy makers this responsibility rests upon them. According to Mirella, it is important for the top management to maintain focus and vision by actively engaging in both mandatory periodic reviews and non-routine checks on the efficacy of the installed systems, infrastructure, policies and procedures.[78] The study thus deducts that top management information security reviews are critical in the overall protection of the institutional ICT infrastructure, stability, integrity, information safety, operational efficiency, consistency, reliability and against third party intrusions.[79]

### 4.3.11 Hypothesis Testing

The specific objective of the study was to identify the information security measures required to protect the e-government services in Kenya. The following hypothesis was tested at a significance level of 5% (0.05) using the SPSS software:

**H0:** The types of information security measures have no effect on the quality of e-government services in Kenya.

---

[77] Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.

[78] Sutopo, Bambang, Trisninik Ratih Wulandari, Arum Kusumaningdyah Adiati, and Dany Adi Saputra. "E-government, audit opinion, and performance of local government administration in Indonesia." *Australasian Accounting, Business and Finance Journal* 11, no. 4 (2017): 6-22.

[79] Gheorghe, Mirela. "Audit Methodology for IT Governance." *Informatica Economica* 14, no. 1 (2010).

**H1:** The types of information security measures have significant effect on the quality of e-government services in Kenya.

**$Chi^2$ –Test = $x^2$ , df 9 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 18.39**

The $Chi^2$ –Test of 18.39 is significantly greater than the critical value of 16.92 at 5% significant level. We thus reject the Null Hypothesis (H0) and accept the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya.

### 4.3.12 Chapter Summary

The summary findings from this chapter indicates that out of 1200 questionnaires sent out to the target population 966 respondents filled and returned the questionnaires making a response rate of 80%. The research response rate of 50% is considered adequate, rate of 60% is considered good and any rate above 70% is considered excellent. The information security preventive measures data results strongly indicates that 1719 respondents returned negative responses at 9% and 7941 respondents returned positive response at 91%. 13% disagreed while 87% largely agreed that national legislations is a pre-requite for establishing protective framework. 16% disagreed while 84% largely agreed that policies, plans and strategies are important. 19% disagreed while 81% largely agreed that ICT training for the institutional operators, vendors and service providers was important institutional capacity building.

The study further made a finding that summative 20% disagreed while 80% largely agreed that physical security, use of codes, authentic passwords and user procedures and protocols are essential to enhance integrity of the e-government systems. Further, 20%

disagreed while 80% largely agreed that frequent audits of ICT systems, infrastructure and procedures is an important function. 19% disagreed while 81% largely agreed that installations of hardware and system back ups are important protection and safeguard measures. 16% disagreed while 84% largely agreed that installations of system security firewalls and automated monitoring intelligence are important protection and safeguard measures.

The study further made a finding that 19% disagreed while 81% largely agreed that top management information security reviews are important protection and safeguards measures against the information security threats that face e-government services in Kenya. The **Chi$^2$ –Test** of 18.39 > 16.92 was significantly greater at 5% significant level rejecting the Null Hypothesis (H0). Thus the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya was accepted.

# CHAPTER FIVE: SUMMARY FINDINGS AND RECOMMENDATIONS

## 5.1 Introduction

This chapter presents the summary findings and analysis presented in chapter two, chapter three and chapter four. The chapter finally presents the conclusion and recommendations.

## 5.2 Summary of the Findings

The study made the following findings on the population characteristics, government services, information security threats and the preventive measures against information security threats to the provision of e-government service in Kenya. The data was compiled from the study questionnaires issued to the respondents. The questionnaire comprised both closed and open-ended questions. This data has been analysed using Statistical Package for Social Sciences (SPSS). The research findings have been presented in tables, figures, graphs, frequency distributions and descriptive statistics.

### 5.2.1 Demographic Data

From the findings, 78.78% of respondents were males, 19.19% females and 3.3% from other genders. This shows that the study had more males than females. Age distribution was analyzed as follows; Ages 15-25 years old 5.5%, ages 26-35 years old 18.18%, ages 36-50 years old 52.52% and ages 51 years and above 25.25%. This was a good indication that the respondents provided relevant information covered in the questionnaire. Based on this finding, the respondents had acquired formal education as follows; Primary Education 9%, Secondary Education 31%, and Graduate Education 60%. The study noted that majority had acquired formal education at a level of 90% which was an excellent

requirement for the research. Based on this findings, 822 respondents about 85% were Kenyans while 144 respondents about 15% were foreigners.

The study thus managed to obtain data from both nationals and foreigners. This is important because government services are provided to both nationals and non-nationals. The findings indicate that 80% of respondents have lived in Kenya for more than 10 years, 10% have been in Kenya for a period of between 5-10 years and another 10% have been in the country for less than 5 years. Period of residence by the respondent was of interest to the study because it correlates to the experience of respondents with the services offered by the Kenya government.

The study found that Kenyan citizens were the majority at 50%, followed by Kenyan registered Companies at 35%, then Foreign Citizen individuals at 5% and Foreign Agencies 10%. The category of the respondents was of interest to the study since this would provide a good indicator of their personal interaction and experience with the government services in Kenya. From the findings, 95% of respondents have sought for public services in Kenya while 5% had not. This is a positive indicator towards the achievement of the objective of the study.

Based on these findings, 415 respondents representing 43% were citizens who sought government services (G2C), 339 respondents representing about 35% sought Government to Business (G2B) services, 19 respondents representing 2% sought Government to Government services and 193 respondents representing 20% sought Government to

employees services. The study thus managed to obtain data from both nationals and foreigners. From the findings above, of the respondents who sought public services, only 3% obtained them through a manual system, 47% transacted through a digital/online platform and 50% obtained them through a mixed manual/digital interface. This is a positive indicator that the majority of respondents obtained public services through a digital platform.

#### 5.2.1.1 Hypothesis Testing

**$Chi^2$ –Test = $x^2$ , df 3 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 10.83**

The $Chi^2$ –Test of 10.83 is significantly greater than the critical value of 9.35 at 5% significant level. We thus reject the Null Hypothesis (H0) and accept the Alternative Hypothesis (H1) that the type of services have significant effect on the quality of e-government services.

### 5.2.2 Information Security Threats to E-government Services

#### 5.2.2.1 The unauthorized access and interference with system networks

The study found that 6.83% Strongly Disagreed, 8.59% Disagreed, 13.15% Neither Agreed nor Disagreed, 44% Agreed and 27.12% Strongly Agreed. The study further made a finding that summative 28% largely disagreed and 72% equally agreed that unauthorized system access remained a significant security threat to government e-government services.

#### 5.2.2.2 Illegal Devices

The study found that 7.87% Strongly Disagreed, 11.08% Disagreed, 16.15% Neither Agreed nor Disagreed, 39.13% Agreed and 25.78% Strongly Agreed. The study further made a finding that summative 19% largely disagreed and 81% equally agreed that illegal devices remain a significant security threat to e-government services

#### 5.2.2.3 Unauthorized Codes and Password

The study found that 9.63% Strongly Disagreed, 7.87% Disagreed, 19.77% Neither Agreed nor Disagreed, 38.30% Agreed and 24.43% Strongly Agreed. The study further made a finding that summative 18% largely disagreed and 82% equally agreed that unauthorized codes and passwords remain a significant security threat to e-government services.

#### 5.2.2.4 False Publications

The study found that 6.11% Strongly Disagreed, 11.70% Disagreed, 15.94% Neither Agreed nor Disagreed, 38.51% Agreed and 27.74% Strongly Agreed. The study further made a finding that summative 18% largely disagreed and 82% equally agreed that False Publications remain a significant security threat to e-government services.

#### 5.2.2.5 Computer Frauds and Forgery

The study found that 8.39% Strongly Disagreed, 6.0% Disagreed, 8.80% Neither Agreed nor Disagreed, 34.68% Agreed and 42.13% Strongly Agreed. The study further made a

finding that summative 14% largely disagreed and 86% equally agreed that computer frauds and forgery remain a significant security threat to e-government services.

5.2.2.6 Cyber espionage, terrorism and squatting

The study found that 6.83% Strongly Disagreed, 6.830% Disagreed, 16.56% Neither Agreed nor Disagreed, 35.40% Agreed and 34.37% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that cyber espionage, terrorism and squatting were serious security threat to e-government platforms and services delivery.

**5.2.2.7 Phishing**

The study found that 8.18% Strongly Disagreed, 7.35% Disagreed, 16.15% Neither Agreed nor Disagreed, 40.58% Agreed and 27.74% Strongly Agreed. The study further made a finding that summative 15% largely disagreed and 85% equally agreed that phishing was a serious security threat to e-government platforms and services delivery.

**5.2.2.8 Identity theft and impersonation**

The study found that 6.83% Strongly Disagreed, 6.83% Disagreed, 12.63% Neither Agreed nor Disagreed, 38.51% Agreed and 35.20% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that identity theft and impersonation were a serious security threat to e-government platforms and services delivery.

#### 5.2.2.9 Interception of electronic messages and money transfer

The study found that 7.66% Strongly Disagreed, 6.83% Disagreed, 16.36% Neither Agreed nor Disagreed, 33.95% Agreed and 35.20% Strongly Agreed. The study further made a finding that summative 15% largely disagreed and 85% equally agreed that interception of electronic messages and money transfer was a serious security threat to e-government platforms and services delivery.

#### 5.2.2.10 Fraudulent use of electronic data

The study found that 7.35% Strongly Disagreed, 6.83% Disagreed, 10.04% Neither Agreed nor Disagreed, 40.58% Agreed and 35.20% Strongly Agreed. The study further made a finding that summative 14% largely disagreed and 86% equally agreed that fraudulent use of electronic data was a serious security threat to e-government platforms and services delivery.

#### 5.2.2.11 Employee irresponsibility, aiding and abetting offences

The study found that 10.04% Strongly Disagreed, 7.25% Disagreed, 12.32% Neither Agreed nor Disagreed, 36.85% Agreed and 33.54% Strongly Agreed. The study further made a finding that summative 17% largely disagreed and 83% equally agreed that employee irresponsibility, aiding and abetting offences is serious security threat to e-government platforms and services delivery.

#### 5.2.2.12 Child Pornography

The study found that 15.63% Strongly Disagreed, 11.49% Disagreed, 22.15% Neither Agreed nor Disagreed, 27.64% Agreed and 23.08% Strongly Agreed. The study further made a finding that summative 27% largely disagreed and 73% equally agreed that child pornography is serious security threat to e-government platforms and services delivery.

#### 5.2.2.13 Hypothesis Testing

**$Chi^2$ –Test = $x^2$ , df 11(n-1) = $\sum (Oi - Ei)^2 / Ei$ = 20.47**

The $Chi^2$ –Test of 20.47 is significantly greater than the critical value of 19.68 at 5% significant level. We thus reject the Null Hypothesis (H0) and accept the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya.

.

### 5.2.3 Preventive Measures against threats

The measures were grouped in 10 categories of threats tabulated above. 551 respondents strongly disagreed, 262 respondents disagreed, 907 respondents neither agreed nor disagreed, 2731 respondents agreed and 5210 respondents strongly agreed. The data results strongly indicates that 1719 respondents returned negative responses at 9% and 7941 respondents returned positive response at 91%. The measures are summarized below:

#### 5.2.3.1 National Legislations

The study found that 6% of the respondents Strongly Disagreed, 3% Disagreed, 7% Neither Agreed nor Disagreed, 35% Agreed and 48% Strongly Agreed. The study further made a finding that summative 13% disagreed while 87% largely agreed that national legislations is a pre-requite for establishing protective framework against the information security threats that face the e-government services delivery in Kenya.

#### 5.2.3.2 Institutional policies, plans and strategies

The study found that 6% of the respondents Strongly Disagreed, 2% Disagreed, 8% Neither Agreed nor Disagreed, 32% Agreed and 53% Strongly Agreed. The study further made a finding that summative 16% disagreed while 84% largely agreed that policies, plans and strategies are important institutional framework essential to guarantee protection against the information security threats that face the e-government services delivery in Kenya.

#### 5.2.3.3 ICT Training

The study found that 5% of the respondents Strongly Disagreed, 5% Disagreed, 9% Neither Agreed nor Disagreed, 25% Agreed and 56 % Strongly Agreed. The study further made a finding that summative 19% disagreed while 81% largely agreed that ICT training for the institutional operators, vendors and service providers was important institutional capacity building to guarantee protection against the information security threats that face the e-government services delivery in Kenya.

#### 5.2.3.4 Installation of end to end back up security

The study found that 5% of the respondents Strongly Disagreed, 1% Disagreed, 9% Neither Agreed nor Disagreed, 25% Agreed and 60% Strongly Agreed. The study further made a finding that summative 15% disagreed while 85% largely agreed that installation of end to end back up security was important institutional procedural undertaking and capacity building to guarantee protection against the information security threats that face the e-government services delivery in Kenya.

#### 5.2.3.5 Physical security, codes, passwords and control protocols

The study found that 6% of the respondents Strongly Disagreed, 4% Disagreed, 6% Neither Agreed nor Disagreed, 25% Agreed and 55% Strongly Agreed. The study further made a finding that summative 20% disagreed while 80% largely agreed that physical security, use of codes, authentic passwords and user procedures and protocols was important to guarantee protection against the information security threats that face the e-government services in Kenya.

#### 5.2.3.6 Employment of professionally certified staff

The study found that 5% of the respondents Strongly Disagreed, 4% Disagreed, 15% Neither Agreed nor Disagreed, 32% Agreed and 44% Strongly Agreed. The study further made a finding that summative 24% disagreed while 76% largely agreed that employment of professionally certified staff in the ICT function is a critical requirement to guarantee protection against the information security threats that face the e-government services.

#### 5.2.3.7 Frequent audits of ICT infrastructures, systems, regulations and procedures

The study found that 6% of the respondents Strongly Disagreed, 1% Disagreed, 10% Neither Agreed nor Disagreed, 25% Agreed and 55% Strongly Agreed. The study further made a finding that summative 20% disagreed while 80% largely agreed that frequent audits of ICT systems, infrastructure and procedures is an important function to guarantee the institutional protection against the information security threats that face e-government services in Kenya.

#### 5.2.3.8 Installations of hardware and software backups

The study found that 6% of the respondents Strongly Disagreed, 2% Disagreed, 11% Neither Agreed nor Disagreed, 26% Agreed and 55% Strongly Agreed. The study further made a finding that summative 19% disagreed while 81% largely agreed that installations of hardware and system software back ups are important protection and safeguards against the information security threats that face e-government services in Kenya.

#### 5.2.3.9 Installations of system security firewalls and automated monitoring

The study found that 6% of the respondents Strongly Disagreed, 3% Disagreed, 7% Neither Agreed nor Disagreed, 25% Agreed and 59% Strongly Agreed. The study further made a finding that summative 16% disagreed while 84% largely agreed that installations of system security firewalls and automated monitoring intelligence are important protection and safeguards against the information security threats that face e-government services in Kenya.

#### 5.2.3.10 Top Management Information Security Reviews

The study found that 6% of the respondents Strongly Disagreed, 2% Disagreed, 11% Neither Agreed nor Disagreed, 28% Agreed and 53% Strongly Agreed. The study further made a finding that summative 19% disagreed while 81% largely agreed that top management information security reviews are important protection and safeguards against the information security threats that face e-government services in Kenya.

#### 5.2.3.11 Hypothesis Testing

**$Chi^2$ –Test = $x^2$ , df 9 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 18.39**

The $Chi^2$ –Test of 18.39 is significantly greater than the critical value of 16.92 at 5% significant level. We thus reject the Null Hypothesis (H0) and accept the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya.

## 5.3 Conclusion

During the last decade, the Kenya government has progressively adopted e-governance systems embracing digital online services for provision of public services and collection of government revenues. The challenges and opportunities brought about by globalisation which has revolutionized interconnectivity and interdependence through astronomical advances in information and communication technology and internet connectivity systems. This makes the world's political, economic, cultural and social interactions extremely vulnerable to vicious threats from the operating virtual environment within largely diminishing state control and sovereignty challenges.

This study set out to examine the information security threats to e-government services in Kenya. The study was guided by both the General Systems and globalisation theories and adapted descriptive research methodology. The study target population was users and service providers from the 51 Huduma Service Centres in Kenya. The sample size was 10% purposive sampling techniques was applied to 10 Huduma Service Centres in the country targeting all service users and government service agents. The study issued 1200 questionnaires to respondents out of which 966 were returned making a successful response rate of 80%.

The study conceptualized three specific objectives, derived relevant research questions which were successfully administered through a structured questionnaire. The first category of questions sought to determine if the types of public services had any significant effect on the quality of e-government services. The hypothesis test of significance **$Chi^2$ –Test = $x^2$ , df 3 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 10.83 > 9.35 at 5% significant level**. The study thus rejects the null hypothesis (H0) stating that the type of public services have no effect on the quality of e-government services and accept the Alternative Hypothesis (H1) that the type of services have significant effect on the quality of e-government services.

The second category sought to identify the types of security threats and their effect on the quality of e-government services. The hypothesis test of significance **$Chi^2$ –Test = $x^2$ , df 11 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 20.47 > 19.68 at 5% significant level**. The study thus

rejects the null hypothesis(H0) stating that the information security threats have no effect on the quality of e-government services and accept the Alternative Hypothesis(H1)

The third category of questions sought to identify the information security safeguard measures and if they had any significant effect on the quality of e-government services. The sample tests of significance **$Chi^2$ –Test = $x^2$ , df 9 (n-1) = $\sum (Oi - Ei)^2 / Ei$ = 18.39 > 16.92 at 5% significant level**. The study thus rejects the null hypothesis (H0) stating that the information security threats have no effect on the quality of e-government services and accepts the Alternative Hypothesis (H1) that the information security threats have significant effect on the quality of e-government services in Kenya.

## 5.4 Recommendations

Globalization and revolutions in destructive Artificial Intelligence digital technologies and cyberspace have brought many benefits as well as greater information security threats to the conduct of international politics, commerce, public services and social cultural interactions due to increased connectivity and interdependence significantly impairing national security and sovereignty. The developing nations such as Kenya face severe operational and security challenges for heavy dependency on imported technologies and infrastructure support systems. To overcome these contemporary global challenges, the study strongly recommends home-made technological solutions, naturing of local digital technology hubs and innovation centres, strong policy measures in government ICT cyber security management, international collaboration, frequent infrastructure security monitoring and upgrades, employees and user capacity training, reviews and upgrades in tandem to the evolving information security threats and threats management. Further

research is recommended on the impact of information security threats on political, economic and social activities in Kenya as the country migrates steadily into digital knowledge economy embracing integrated e-citizen public and commercial services within the volatile cyberspace with limited sovereign control, preventive, defensive and offensive capabilities. There is also need for the country to re-organize and restructure the national security and defence institutions and critical infrastructure to guarantee national security, safety, accessibility, integrity, confidence, privacy and redundancy of national data and information.

## REFERENCES


Albrow, Martin; King, Elizabeth Globalisation, Knowledge and Society. London: Sage. (1990), pp. 300-315.

Amoretti, Francesco. "International organizations ICTs policies: e-democracy and e-government for political development." *Review of policy research* 24, no. 4 (2007): 331-344.

Anderson, Monica. Mobile Technology and Home Broadband, 2019. Pew Research Center.

AU AGENDA 2063 (2015), https://au.int/en/agenda2063/overview, Accessed on 20th August 2021 at 1246 pm

Bergquist, K., Fink, C., & Raffo, J. Global Innovation Index 2018: Energizing the World with Innovation. Geneva: Cornell, 2018, and WIPO. 193–209.

Camastra, Francesco, Angelo Ciaramella, and Antonino Staiano. "Machine learning and soft computing for ICT security: an overview of current trends." *Journal of Ambient Intelligence and Humanized Computing* 4 (2013): 235-247.

Chanchala, Joshi, and Singh, Umesh Kumar. *"Information security risks "*. Journal of Information Security and Applications. (June, 2017), 35: 128–137.

Ciampa, M. Security Awareness: Applying practical Security in your world. Boston:, MA Cengage 2018

Clement, J. (2019). "Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)." Statista, August 5, 2019. Retrieved from https:www. Statista.com/statistics.

Craig R. Scott and Laurie Lewis, The International Encyclopedia. The International Encyclopedia of Organizational Communication. (London: John Wiley & Sons ,2018), 106. cybersecurity-threat-burden-and-role-of-tax-practitioners

Creswell, John W., and J. David Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017

Creswell,W. J. (2007). Qualitative Inquiry and Research Design: Choosing Among Five Approaches, London: Sage Publications.

Creswell. J.W. and Creswell, J.D. (2017) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition, Sage, Newbury Park

Dahlman, Carl, Sam Mealy, and Martin Wermelinger. "Harnessing the digital economy for developing countries." (2016).

Elmi, N. (2021). Digitilising tax, The Kenyan way, The travels and translations of iTax in Kenya. Linkoping University.

Farina, Rose. Securing what you don't own or have. Washington DC: Oxford University Press, 2019.

Fung, B. (2018). Equifax's massive 2017 data breach keeps getting worse. Washington Post, March 1, 2018, 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-peoplewho-were-affected-by-its-massive-data-breach/?noredirect=on. Accessed February 8, 2020.

Gheorghe, Mirela. "Audit Methodology for IT Governance." *Informatica Economica* 14, no. 1 (2010).

Glikson, Ella, and Anita Williams Woolley. "Human trust in artificial intelligence: Review of empirical research." *Academy of Management Annals* 14, no. 2 (2020): 627-660.

Government of Kenya, The Constitution, 2010, http://kenyalaw.org/kl/index.php?id=398. Accessed on 14 August, 2022 at 1130 pm.

Government of Kenya, Vision 2030 (2015), https://vision2030.go.ke/, Accessed on 20th August 2021 at 1246 pm

Hira, Tahira K., and Olive M. Mugenda. "The relationships between self-worth and financial beliefs, behavior, and satisfaction." *Journal of family and consumer sciences* 91, no. 4 (1999): 76

Irani, Zahir, Peter ED Love, and Ali Montazemi. "E-government: past, present and future." *European Journal of Information Systems* 16, no. 2 (2007): 103-105.

James, Paul and Steger, Manfred B. A Genealogy of globalisation: The career of a concept, Globalisations, 2014, **11** (4): 417–34.

Janine, Kremling, Amanda, M., Sharp Parker. Cyberspace, Cybersecurity and Cybercrime. London: SAGE Publications, 2018.

Joshi, Chanchala; Singh, Umesh Kumar. *"Information security risks management framework – A step towards mitigating security risks in university network"*. Journal of Information Security and Applications.2017, **35**: 128–137.

Kenya National Bureau of Statistics, Communications Authority of Kenya (2016). Enterprise ICT Survey 2016. Retrieved from: https://ca.go.ke/wp content/uploads/2018/02/Enterprise-ICT-Survey-Report-2016.pdf

Krasner, Stephen D. *Defending the national interest: Raw materials investments and US foreign policy*. Vol. 1. Princeton University Press, 1978. Khisa, M., Odima, Z., Wafula, R.,

Innovative Ways the Government of Kenya is Delivering Services to its Citizens through E-Government. School of Computing and Informatics, University of Nairobi 2020

Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International journal of critical infrastructure protection* 25 (2019): 36-49.

Kothari, C. R., & Garg, G. Research Methodology: Methods and Techniques. New Delhi: New Age International Publishers, (2014).

Kothari, C.R. (2005), *" Research Methodology: Methods and Techniques"* New Age PublishersMarsh.D. and & Stolker, G. ( 2010) Theory and Methods in Political Science. London: Palyave Macmillan.

Kremling, Janine., Amanda, M., Sharp Parker. Cyberspace, Cybersecurity and Cybercrime. (London: SAGE Publications, 2018), 110.

López-Bassols, Vladimir. "ICT skills and employment." (2002).

Martin Hilbert and Priscila López. The World's Technological Capacity to Store, Communicate, and Compute Information, Science, 2011, 332 (6025), pp. 60-65.

Montuori, A. Systems Approach. *Encyclopedia of Creativity*, Academic Press, 2011, Pp. 414–21

NIST Special Publication (SP) 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2016, p 307.

Olive M. Mugenda and Abel G. Mugenda : Research Mentods: Quantitative and Qualitative Approaches. (Nairobi: ACTS, 2003), PP. 42.

Owigar, J. & Omwenga, E.I. User-centric evaluation, ( *International Journal of Computer Applications,2018)*, 148 (8):17-23.

Owigar, J.A. & Omwenga, E.I. (2019). User-centric evaluation of Government of Kenya online services: The case of iTax, *International Journal of Computer Applications,*148 (8):17-23

Poole, M. S. Systems theory. In L. L. Putnam & D. K. Mumby (Eds.), The SAGE handbook of organizational communication: Advances in theory, research, and methods, CA: Sage , 2014, pp. 49–74.

Retrieved from https://news.bloombergtax.com/daily-tax-report/insight-the-

Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." *Computers & security* 49 (2015): 70-94.

Rose, Farina. Securing what you don't own or have. (Washington DC: Oxford University Press, 2019), pp.230-232.

Shafqat, Narmeen, and Ashraf Masood. "Comparative analysis of various national cyber security strategies." *International Journal of Computer Science and Information Security* 14, no. 1 (2016): 129-136.

Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage. Cyber Crime, Cyber Space and Effects of Cyber Crime. Volume 7, Issue 1 Page Number: 210-214 Publication Issue : January-February-2021

Sutopo, Bambang, Trisninik Ratih Wulandari, Arum Kusumaningdyah Adiati, and Dany Adi Saputra. "E-government, audit opinion, and performance of local government

administration in Indonesia." *Australasian Accounting, Business and Finance Journal* 11, no. 4 (2017): 6-22.
UN E-GOVERNMENT SURVEY (2020), publicadministration.un.org, Accessed on 20th August 2021 at 1246 pm
United Nations, Department of Economic and Social Affairs. https://unstats.un.org/sdgs, accessed on 20th August at 1246 pm.
Valentina (Dardha) Ndou. E – government for developing countries: opportunities and challenges. Ejisdc (2004) 18, 1, 1-24. Http://www.ejisdc.org
Wausi, Njihia & Kamau (2016). E-government websites user experience from public value perspective: Case study of iTax website in Kenya. Conference: 2016 IST-Africa Conference.
Wells, G. Insight: The cybersecurity threat, burden, and role of tax practitioners, 2019.
Wolf, Martin. Shaping Globalisation. Washington DC: International Monetary Fund, 2014. Accessed on 20 August 2022, 51.

## APPENDIXES

### APPENDIX 1: LETTER OF INTRODUCTION

GODFRED OHNDYL OTHIENO
P O BOX 10345-00200
NAIROBI, Tel: 0722815461
October 2022

Dear Sir/Madam,

**RE: RESEARCH QUESTIONNAIRE**

I am a post graduate student at National Defence University Kenya (NDU-K) pursuing a **Master's degree in National Security and Strategy.**

As part of academic requirement for the award of the degree, I am undertaking a research study on **"INFORMATION SECURITY THREATS TO E-GOVERNMENT SERVICES IN KENYA ".** The United Nation (UN) through the Digital Government in the Decade of Action for Sustainable Development has encouraged world governments to embrace digital technology popularly known as e-governance in provision of public services. Some of these services includes civil registration, licencing, property rights certificates, payments and collection of revenue. Adoption of ICT is a catalyst towards government efficiency, effectiveness, reduced bureaucracy and many acts of government corruption. The implementation of digital economies in developing world is however faced with many contemporary security threats in all forms of cyber crimes by technical cyber fraudsters. This new global virtual society has negatively affected the sovereignty, territorial integrity and political independence of the modern state which require credible comprehensive security plans and architecture to survive in the new volatile and complex international system.

This research is modelled on **Kenya Government E-CITIZEN services, KRA i-tax, IFMIS and operation of HUDUMA ONE STOP Centres**. The questionnaire voluntarily seeks information pertaining to the study and will be treated with the highest standards of research ethics and confidentiality. The information obtained will not be distributed nor shared with un-authorized person or agency.

Kindly take a few minutes to fill the questionnaire to the best of your knowledge and experience. I am available to clarify on any arising issue via my cell phone +254722815461 or email ondylgo@gmail.comYour assistance will be highly appreciated.

Thank you

Yours faithfully,

Godfred O Ohndyl

## APPENDIX 2: FIELD QUESTIONNAIRE

This questionnaire is designed to collect information that will help the study to identify and analyse the information security threats to the implementation and operation of e-government services in Kenya. The questionnaire has **five sections marked A(Q1-Q6), B(7Q-10Q), C(Q11-Q12), D (13-Q14), E(Q15-Q16) and F (Q17) with serialized questions from 1-17**. Please be honest and objective in completing the sections using the given guidelines within the sections. The information provided shall be strictly used for academic purposes only and will be treated with the highest integrity and utmost confidentiality. You can either tick/mark in the provided spaces or write your responses below the question asked.

### SECTION A: DEMOGRAPHIC DATA

**(Please respond by placing a tick against one of the options provided after the questions)**

1. Please indicate your gender / sex Male ☐ Female ☐

2. How old are you? 15-25 ☐ 26-35 ☐ 36-50 ☐ 51 & Above ☐

3. What is your level of education?

| Higher Education | Secondary | Primary | Nil Education |
|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ |

4. What is your nationality?

| Kenyan | Non-Kenyan |
|---|---|
| ☐ | ☐ |

5. How long have you lived/worked in Kenya?

| Less than 5 Yrs | Between 5-10 Yrs | Between 10-15 Yrs | More Than 15 Yrs |
|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ |

6. What is your category/ organization?

Kenyan Individual ☐ Kenyan Company ☐ Foreign Individual ☐ Foreign Agency ☐

**SECTION B: KENYA GOVERNMENT SERVICES**

7. Have you ever sought government services in Kenya?

Yes ☐ No ☐

8. What was the type of services?

☐ Government to Citizen { (G2C) Civil Registrations, Property, general services}

☐ Government to Business { (G2B) Licences, Revenues, Taxations, Permits}

☐ Government to Government {(G2G) Private and commercial}

☐ Government to Employees {(G2E) Salaries, Reports, instructions, Returns}

9. What was the method or platform used?

☐ Manual

☐ Digital Electronic/ Online

10. Rate the quality of service?

☐ Excellent

☐ Good

☐ Average

☐ Not Good

☐ Worse

## SECTION C: TYPES OF INFORMATION SECURITY THREATS

**(Please respond by placing a tick against one of the options provided by the five point Linkert scale below)**

11. The following are the types of information security threats to e-government services in Kenya. Please indicate the extent to which you agree or disagree with each.

**1 = Strongly disagree**
**2 = Disagree**
**3 = Neither agree nor disagree**
**4= Agree**
**5 = strongly agree**

| | **Types of Information Security Threats** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| a | Unauthorized access, interference and interference | | | | | |
| b | Illegal devices | | | | | |
| c | Unauthorized codes and passwords | | | | | |
| d | False publications | | | | | |
| e | Computer frauds and forgery | | | | | |
| f | Cyber espionage | | | | | |
| g | Cyber terrorism | | | | | |
| h | Cyber harassment and squatting | | | | | |
| i | Phishing | | | | | |
| j | Identity theft and impersonation | | | | | |
| k | Interception of electronic messages and money transfer | | | | | |
| l | Fraudulent use of electronic data | | | | | |
| m | Employee irresponsibility, aiding or abetting offences | | | | | |
| N | Child pornography | | | | | |

12. List below other types of information security threats to e-government services that have not been mentioned above……

## SECTION D: IMPACTS OF INFORMATION SECURITY THREATS

**(Please respond by placing a tick against one of the options provided after the questions)**

13. The following are the impacts of information security threats to e-government services in Kenya. Please indicate the extent to which you agree or disagree with each.

**1 = strongly disagree**
**2 = Disagree**
**3 = neither agree nor disagree**
**4= Agree**
**5 = strongly agree**

| | Consequences of information security threats | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| a | Unauthorized access | | | | | |
| b | Alterations, modifications, deletion and destruction of data, information and programmes | | | | | |
| c | Cybercrimes, cyber squatting and cyber terrorism | | | | | |
| d | Interference, interception and theft of data information and financials | | | | | |
| e | Network seizure, service denial and disruptions | | | | | |
| f | Compromised data confidentiality, integrity, access and availability | | | | | |
| g | Loss of privacy and intrusion of personal freedoms | | | | | |
| h | Theft of data, files, information and technology | | | | | |
| i | Destruction of critical information infrastructure | | | | | |
| j | Theft and loss of digital money, messages and information | | | | | |
| k | Damages to corporate image | | | | | |
| l | Unlawful processing of personal and corporate data | | | | | |

14. List below other impacts of information security threats to e-government services that have not been mentioned above.

## SECTION E: PREVENTIVE MEASURES AGAINST INFORMATION SECURITY THREATS

**(Please respond by placing a tick against one of the options provided after the questions)**

15. The following are the preventive measures against information security threats to e-government services. Please indicate the extent to which you agree or disagree with each

**1 = strongly disagree;**
**2 = Disagree;**
**3 = neither agree nor disagree;**
**4 = Agree;**
**5 = strongly agree**

| | **Preventive measures against information security threats** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| a | National legislations on information security is required | | | | | |
| b | Implement institutional policies, plans and strategies | | | | | |
| c | ICT training for service providers, vendors, operators and users is important | | | | | |
| d | Install end to end and back up computer security | | | | | |
| e | Enforce physical security, passwords and codes security control protocols for all users | | | | | |
| f | Employment and utilization of professional staff with appropriate certifications | | | | | |
| g | Frequent audits of ICT infrastructure, systems, programmes, procedures and regulations | | | | | |
| h | Install ICT hardware and software backups solutions and power systems | | | | | |
| i | Install computer and information security firewall and surveillance monitoring | | | | | |
| j | Top management information security reviews | | | | | |

16. List below other measures that can be taken to prevent information security threats to e-government services……

## SECTION F: RESPONDED GENERAL OPINION

17. Do you have any comments or opinions or suggestions to improve this study on information security to e-government services in Kenya?

**THANK YOU FOR YOUR TIME AND COOPERATION**

**-END-**

## APPENDIX III: Time Frame of Study 2022-2023

| ACTIVITY | PERIOD ( MONTHS) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | SEP'22 | SEP'22 | SEP'22 | OCT'22 | OCT'22 | DEC'22 | DEC'22 | JAN'23 | FEB 2023 | MAR' 2023 | APR 2023 |
| Draft proposal & presentation | | | | | | | | | | | |
| Presentation & correction of draft report | | | | | | | | | | | |
| Defense | | | | | | | | | | | |
| Correction & refinement | | | | | | | | | | | |
| Data collection | | | | | | | | | | | |
| Data entry & analysis | | | | | | | | | | | |
| Report Writing | | | | | | | | | | | |
| Draft Report | | | | | | | | | | | |
| Supervisors Review | | | | | | | | | | | |
| Final submission | | | | | | | | | | | |