Global Journals LATEX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

CrossRef DOI of original article:

Information Security Threats to e-government Services in Kenya

James J Kimuyu,

Received: 1 January 1970 Accepted: 1 January 1970 Published: 1 January 1970

Abstract

This study examined information security threats to e-government services commonly known as e-citizen. Grounded on General Systems Theory examined the nature of complex inter-relationships and interdependence of global society, states, non-state actors and individuals and how they relate in a complex internet â??"enabled communication network. Mixed method cross sectional survey was used. Targeted population of 12000 respondents from 51 Huduma Centres. Purposive sampling at 10

Index terms— competition, cyber, e-citizen, information, threats, interdependence.

1 Introduction

he digital transformation and increasing development of applications within the Information Communication Technology (ICT) industry has been quite astronomical within the 21 st 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. (Kremling et al?2018) 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, redundant and low investments in research and development programmes, 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. **??**Farina, 2019) In 2015, the United Nations (UN) rolled out the Agenda 2030 for sustainable development of the world following the purposed achievement of Millennium Development Goals (MDGs). The International Governmental Organization (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. (UN, SDG, 2015). All these initiatives embraces the development of world knowledge economy framed on ICT.

The UN as a global agenda setter through policy support initiatives continues to encourage 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. (UN, 2020) At the continental level, the African Union (AU) Agenda 2063 framework, further seeks to consolidate the socialeconomic 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 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. **??**AU, 2015) 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. (GoK Constitution, 2010) 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 **??**GoK, 2015).

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 with vision to reach about 5000 services in future. 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 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. (KNBS, 2016). These 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 and heavy dependency and reliance on imported technology and infrastructure support systems from leading world multinational corporations (MNCs) (Ciampa, 2018).

The number of businesses that have experienced data breaches has grown exponentially during this 21 st 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. (Clement, 2019). 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.

2 a) 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 commerce and delivery of public services by modern nation states (Dahlman et al?, 2016). 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, distributed denial of services (DDoS) data fraud, equipment destruction and disruption of services (Kimathi et al?2019). 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 (Ella, and Woolley, 2020) Developing nations such as Kenya and mostly the fifth world lack the research and development capabilities for local production and thus remain heavily dependent on imported technological applications and software's from world leading MNCs abroad. These are accompanied with high acquisition costs, old technologies, poor implementation and adoption and mostly fragmented technology support legal framework (Shafqat, 2016).

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, deny, alter or steal institutional or country information and data for 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 that heavily depends on foreign manufactured imported H1: The types of information security threats have significant effect on the quality on e-government services in Kenya.©

3 e) Scope of the study

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

4 II.

5 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.

6 a) Theoretical Framework

The study was guided by Ludwig Von Bertalanffy, General System Theory (GST). This theory has interdisciplinary application and adoption borrowing from biology, engineering, mathematics, sociology, philosophy, political science, organizational studies, communications and information science (Craig R. Scott and Laurie Lewis, 2018). 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 (Montuori, 2011).

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 (Poole, 2014). 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.

7 b) 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.

8 i. Globalisation

The concept of globalisation has been around for a few decades gaining popularity in the 20 th Century. In the 21 st 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 world more connected and interdependent leading to improved movements, trade, commerce and communication. This has significantly reduced time and lowering associated costs (Wolf, 2014). 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 (Albrow et, al?1990) 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 (James and Manfred, 2014).

9 ii. 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 United States, Europe, and Eastern Asia lead the park in science and technology associated with big investments in Research and Development (R&D) programmes (Bergquist, Fink, & Raffo, 2018).

10 iii. 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 (Wells, 2019).

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 (Anderson, 2019).

iv. 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, speed, efficiency, effectiveness, increased transparency, greater convenience, revenue growth, and/or cost reductions (Wells, 2019).

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 egovernment sites are not properly secured (Owigar and Omwenga, 2018). This study sought to examine information security threats to the e-government services in Kenya.

11 v. Information Security

This study focused on importance of information security to a state, organization or to the lowest level of an individual. The state is the major unit of analysis on matters national security to guarantee sovereignty and defence of national interests against externally generated threats (Krasner, 1978). 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 or the state fundamental to key decision making and must therefore be protected viciously. (Joshi, and Kumar. 2017) 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 (Michael, Jones, and Janicke, 2015). 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 (Janine., Amanda, and Parker 2018). The modern time technology and economic wars between the world leading superpowers have led to escalations in cyber security threats where nations continue to build and restructure their national security architecture to take care of the cyberspace by building preventive, defensive and offensive cyber space coercive capabilities (Borghard, and Lonergan, 2017).

12 vi. 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 total of 51 Huduma Centres have since been established and some are still 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. The country just like many developing nations particularly in Africa lacks locally manufactured on developed technology and heavily relies on foreign imports and infrastructure from leading MNCs and holds limited or essential proprietary rights over them. The rising geopolitical competition, collaborations, conflicts and rivalry among the superpowers and world leading industrial nation exposes such installed national infrastructure into foreign cyberspace control and coercion by the technology advanced nations. Thus this study undertook this task to assess the potential information security threats together with their impact on the e-government services in Kenya.

13 Research Methodology a) Research Design

The research design constitutes the blue print for the collection, measurement and analysis of data. (Kothari, 2005). 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 survey.

14 b) Target Population

Target population in statistics is the specific population about which information is desired. (Creswell and Creswell, 2017) 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. (Creswell, 2007) 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 was 12000 respondents being both 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 researcher's resources.

15 c) 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. ??Creswell, 2017) 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 study. ??Creswell and Creswell, 2017)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 (Mugenda and Mugenda, 2003). 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.

16 d) 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 on a five point likert scale 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. ??Creswell, 2011). 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-government platform.

17 e) 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 gave the researcher the opportunity to improve the quality of the research instrument and correction of data collection errors.

18 f) 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. The study used chi-square test and tables to validate the hypothesis Analysis of Variance was used to test the level of significance of the variables on the dependent variable at 95% confidence level ??Creswell and Creswell, 2018).

19 g) 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.

IV.

20 Results and Discussion

21 a) Field Questionnaires issued and responses

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. (Kothari & Garg, 2014) 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. (Tahira and Mugenda, 1999) 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.

22 b) Information Security Threats to E-government Services

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 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:

i. The unauthorized access, service denial (DDoS) 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,(1999) any findings above 70% is considered excellent. Similar studies by Khisa, Odima and Wafula, (2020) identified 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. (Khisa, Odima and Wafula, 2020) ii. 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, (1999) any findings above 70% is considered excellent. (Tahira and Mugenda, 1999) 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.

23 iii. 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, (1999) 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.

24 iv. 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.

25 v. 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,(1999) any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu (2021), identified computer identity fraud as a major impediments to the e-governance systems and services. The study deducts that use of unauthorized codes and passwords are potential security threat which can cause system malfunction and disruption services.

26 vi. 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 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, (1999) any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu, (2021), identified cyber espionage, terrorism and squatting as a major threats to the e-governance systems and services delivery. (Sunil, Pawar, Mente and Bapu, 2021) 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.

27 vii. 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 egovernment platforms and services delivery. According to Tahira and Mugenda, (1999) any findings above 70% is considered excellent. Similar study by Sunil, Pawar and Bapu (2021), 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.

28 viii. 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 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, (2021)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.

29 ix. 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 egovernment platforms and services delivery. According to Tahira and Mugenda, (1999) any findings above 70% is considered excellent. Similar study by Khisa, Odima and Wafula, (2020) identified interception of electronic messages and money transfer as a major threats to the e-governance systems and services delivery. **??** Wafula, 2020) 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.

30 x. 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 egovernance systems and services delivery. 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.

31 xi. 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 egovernment platforms and services delivery. According to Tahira and Mugenda, (1999) any findings above 70% is considered excellent. Similar study by Valentina Ndou (2004), 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. (Valentina Ndou, 2004), The study 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.

xii. 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 egovernance systems and services delivery. (Valentina Ndou, 2004) 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.

32 xiii. 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:

33 c) Hypothesis Test

The specific objective was to investigate the types of insecurity threats that affect the quality of the egovernment 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.

34 H1:

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

35 V. Conclusion and Recommendations a) Conclusion

During the last decade and within the 21 st Century, Kenya government has progressively adopted e-governance systems embracing digital online and telephony services in the provision of public services and collection of national revenues. These successes are happening within a globalizing digital society. These innovations likewise are increasingly attracting new cyber security threats arising from geopolitical competition and rivalries among the super powers and leading industrial nations. The country's heavy dependency and reliance on imported technology from leading MNCs exposes the citizens and national infrastructure to potential cyber security coercion emanating within the cyber space for lack of national capabilities, technological knowhow and expertise within the diminishing state sovereignty and control operating global environment.

This study set out to examine the information security threats to e-government services in Kenya. Guided by General Systems Theory and adapting descriptive research methodology. The study issued 1200 questionnaires out of which 966 were returned making a successful response rate of 80%. The study found that Kenyan citizens were the majority users at 50%, Kenyan registered Companies at 35%, Foreign Agencies 10% and Foreign Citizens at 5%. The services sought comprised; Government to (G2C) 43%, Government to Business (G2B) 35%, Government to employees (G2E) 20% and Government to Government (G2G) 2%. The study identified 12 categories of cyber security threats i.e unauthorized access, illegal devices, unauthorized codes, distributed denial of services (DDoS) false publications, computer frauds, cyber espionage, terrorism and squatting, phishing, identity thefts, electronic interceptions, fraudulent electronic data, employee aiding, child pornography and others. This study further finds that 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. The study equally finds that increased technological inventions, innovations, artificial intelligence capabilities and proliferations has put world superpowers and leading industrial societies at new age of war accusing one another of technology thefts, piracy and cloning. These renewed competition will likely escalate into new collaborative frameworks and conflicts as they seek control dominance, manipulation and exploitative opportunities among each other thus causing significant cyber space challenges and miseries to the developing nations. The hypothesis test at 11 degree of freedom, Chi 2 -Test = x 2 , df 11 (n-1) = ? (Oi -Ei) 2 / Ei = 20.47 > 19.68 at 5% was significantly greater. The study thus rejects the null hypothesis (H0) that the information security threats have no effect on the quality of egovernment services and accepts the Alternative Hypothesis (H1) that information security threats have significant effect on the quality of e-government services.

36 b) Recommendations

In this increasingly globalizing digital economy and shifting global power balance, ownership and leadership in digital technological particularly the immense benefits to be associated with the artificial intelligence capabilities are likely to heighten renewed vicious competitions and rivalries among the superpowers and their allies and with it likely significant technology security challenges for the developing world category in which Kenya belongs. And with clear evidence of declining traditional expeditionary military and mercenary coercive power as witnessed by western powers military campaign failures in Middle East, North Africa, Afghanistan, Ukraine and West Africa its highly likely that the cyberspace will offer the new sphere of influence for the technology giants and thus highly likely increased cyber coercive activities. The study thus recommends that Kenya should develop and invest in local technologies and critical infrastructures, collaborate in international cyber security networks, conduct frequent infrastructure security audits and monitoring, human resource capacity development, implement network security, infrastructure security, applications security, cyber security, cloud security and lastly restructure the national security architecture to provide for national cyber space security capabilities or organs to augment the existing national security architecture in preventive, defensive and offensive capabilities in tandem to the evolving global digital information environment to effectively deter and contain the new security threats emanating geopolitical competition and rivalries among the leading industrial nations.

1

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

Figure 1: Table 1 :

2

Figure 2: Table 2 :

2

is a summary of responden

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.

The normative framework regula

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),

DigitalEconomyKenya'sPolicy

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.

Figure 3: Table 2

4

Frequency	cum%

Figure 4: Table 4 :

.1 Masters Student, National Security & Strategy, National Defence University-Kenya (NDU-K

[Albrow et al. ()] , Martin ; Albrow , Elizabeth King , Globalisation . 1990. London: Sage. p. .

[Washington (2022)] , D C Washington . 20 August 2022. International Monetary Fund. p. 51.

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

[AGENDA ()] , `https://au.int/en/agenda2063/overview` *AGENDA* 2015. AU. 2063. (th August 2021 at 1246 pm)

[Communications Authority of Kenya ()] , *Communications Authority of Kenya* 2016. Kenya National Bureau of Statistics.

[James and Steger ()] 'A Genealogy of globalisation: The career of a concept'. Paul James , Manfred B Steger . *Globalisations* 2014. 11 (4) p. .

[Amoretti ()] Francesco Amoretti . *International organizations ICTs policies: e-democracy and e-government for political development*, 2007. 24 p. .

[Clement (2019)] 'Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)'. J Clement . `www.Statista.com/statistics` *Statista* 2019. August 5, 2019.

[Gheorghe ()] 'Audit Methodology for IT Governance'. Mirela Gheorghe . *Informatica Economica* 2010. 14 (1) .

[Shafqat and Masood ()] 'Comparative analysis of various national cyber security strategies'. Narmeen Shafqat , Ashraf Masood . *International Journal of Computer Science and Information Security* 2016. 14 (1) p. .

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

[Sunil et al. (2021)] *Cyber Crime, Cyber Space and Effects of Cyber Crime*, C Sunil , Dr R S Pawar , Mente , D Bapu , Chendage . 2021. January-February-. 7 p. . (Publication Issue)

[Kimani et al. ()] 'Cyber security challenges for IoT-based smart grid networks'. Kenneth Kimani , Vitalice Oduol , Kibet Langat . *International journal of critical infrastructure protection* 2019. 25 p. .

[Robinson et al. ()] 'Cyber warfare: Issues and challenges'. Michael Robinson , Kevin Jones , Helge Janicke . *Computers & security* 2015. 49 p. .

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

[Valentina et al. ()] 'E -government for developing countries: opportunities and challenges'. (Valentina ,) Dardha , Ndou . `Http://www.ejisdc.org` *Ejisdc* 2004. 18 p. .

[Wausi and Kamau ()] 'E-government websites user experience from public value perspective: Case study of iTax website in Kenya'. Njihia & Wausi , Kamau . *Conference: 2016 IST-Africa Conference*, 2016.

[Sutopo et al. ()] 'E-government, audit opinion, and performance of local government administration in Indonesia'. Bambang Sutopo , Trisninik Ratih Wulandari , Arum Kusumaningdyah Adiati , Adi Dany , Saputra . *Australasian Accounting, Business and Finance Journal* 2017. 11 (4) p. .

[Irani et al. ()] 'E-government: past, present and future'. Zahir Irani , E D Peter , Ali Love , Montazemi . *European Journal of Information Systems* 2007. 16 (2) p. .

[Owigar and Omwenga ()] 'E.I. User-centric evaluation'. J Owigar , Omwenga . *International Journal of Computer Applications* 2018. 148 (8) p. .

[Enterprise ICT Survey ()] *Enterprise ICT Survey*, `https://ca.go.ke/wpcontent/uploads/2018/02/Enterprise-ICT-Survey-Report-2016.pdf` 2016.

[Fung (2018)] 'Equifax's massive 2017 data breach keeps getting worse'. B Fung . `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` *Washington Post* 2018. March 1, 2018, 2018. February 8, 2020.

[Bergquist et al. ()] *Global Innovation Index 2018: Energizing the World with Innovation*, K Bergquist , C Fink , J Raffo , Cornell , Wipo . 2018. Geneva. p. .

[Government ()] Kenya Government . `http://kenyalaw.org/kl/index.php?id=398` *The Constitution*, 2010. (Accessed on 14 August, 2022 at 1130 pm)

[Government ()] Kenya Government . `https://vision2030.go.ke/` *Vision 2030*, 2015. (th August 2021 at 1246 pm)

[Dahlman et al. ()] *Harnessing the digital economy for developing countries*, Carl Dahlman , Sam Mealy , Martin Wermelinger . 2016.

[Glikson and Woolley ()] 'Human trust in artificial intelligence: Review of empirical research'. Ella Glikson , Anita Williams Woolley . *Academy of Management Annals* 2010. 2020. 14 (2) p. .

[López-Bassols ()] *ICT skills and employment*, Vladimir López-Bassols . 2002.

[Chanchala et al. (2017)] 'Information security risks'. Joshi Chanchala , Umesh Singh , Kumar . 10.1016/j.jisa.2017.06.006. *Journal of Information Security and Applications* 2017. June. 35 p. .

[Joshi et al. ()] 'Information security risks management framework -A step towards mitigating security risks in university network'. Chanchala ; Joshi , Umesh Singh , Kumar . 10.1016/j.jisa.2017.06.006. *Journal of Information Security and Applications* 2017. 35 p. .

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

[Wells ()] *Insight: The cybersecurity threat, burden, and role of tax practitioners*, G Wells . 2019.

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

[Kothari ()] C R Kothari . *Research Methodology: Methods and Techniques" New Age Publishers Marsh*, D Stolker , G (eds.) (London) 2005. 2010. Palyave Macmillan.

[Kothari et al. ()] C R Kothari , G Research Garg , Methodology . *Methods and Techniques*, (New Delhi) 2014. New Age International Publishers.

[Krasner ()] S D Krasner . *Defending the national interest: Raw materials investments and US foreign policy*, 1978. Princeton University Press. 1.

[Kremling et al. ()] Janine Kremling , M Amanda , Parker Sharp . *Cyberspace, Cybersecurity and Cybercrime*, (London) 2018. SAGE Publications. p. 110.

[Camastra et al. ()] 'Machine learning and soft computing for ICT security: an overview of current trends'. Francesco Camastra , Angelo Ciaramella , Antonino Staiano . *Journal of Ambient Intelligence and Humanized Computing* 2013. 4 p. .

[Anderson ()] *Mobile Technology and Home Broadband*, Monica Anderson . 2019. Pew Research Center.

[Montuori ()] A Montuori . *Systems Approach. Encyclopedia of Creativity*, 2011. Academic Press. p. .

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

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

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

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

[Rose ()] *Securing what you don't own or have*, Farina Rose . 2019. Washington DC: Oxford University Press. p. .

[Ciampa ()] *Security Awareness: Applying practical Security in your world*, M Ciampa . 2018. Boston: MA Cengage.

[Wolf ()] *Shaping Globalisation*, Martin Wolf . 2014.

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

[Poole ()] 'Systems theory'. M S Poole . *The SAGE handbook of organizational communication: Advances in theory, research, and methods*, L L Putnam , D K Mumby (eds.) 2014. CA: Sage. p. .

[Borghard and Lonergan ()] 'The logic of coercion in cyberspace'. E D Borghard , S W Lonergan . *Security Studies* 2017. 26 (3) p. .

[Hira and Mugenda ()] 'The relationships between self-worth and financial beliefs, behavior, and satisfaction'. Tahira K Hira , Olive M Mugenda . *Journal of family and consumer sciences* 1999. 91 (4) p. 76.

[Hilbert and López ()] 'The World's Technological Capacity to Store, Communicate, and Compute Information'. Martin Hilbert , Priscila López . 10.1126/science.1200970. *Science* 2011. 332 (6025) p. .

[Owigar and Omwenga ()] 'User-centric evaluation of Government of Kenya online services: The case of iTax'. J A Owigar , E I Omwenga . *International Journal of Computer Applications* 2019. 148 (8) p. .