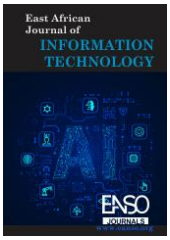

East African Journal of Information Technology
eajit.eanso.org
Volume 7, Issue 1, 2024
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Leveraging Technology for Government Service Delivery: Suggestions for Securing the eCitizen Services in Kenya

Prof. Lucy W. Maina, PhD[1*] *& Godfred Ohndyl Otieno*[2]

[1] Kenyatta University, P. O. Box 43844-00100, Nairobi, Kenya.
[2] International Peace Support Training Centre, P. O. Box 24232 - 00502, Nairobi, Kenya.
* Correspondence ORCID ID: https://orcid.org/0000-0002-8023-2535; email: lucyschola@gmail.com.

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

Date Published:

14 February 2024

Keywords:

Bureaucracy, eCitizen, e-Governance, Information Security, National Sovereignty

ABSTRACT

Governments across the world have increasingly embraced e-governance in the provision of public services. This development has significantly reduced bureaucracy, enhanced efficiency, reduced corruption and fundamentally transformed public service delivery. However, the adoption of these copyright technology solutions, owned by international corporations, non-state actors, mostly multinational corporations (MNCs), have equally exposed user governments, such as Kenya, to significant cyberspace security threats, service disruptions, exposed national security, interferences to national independence and loss of national sovereignty. These threats arise from the activities of offensive states, non-states and individuals taking advantage of the integrated and dependent internet connectivity networks. This paper is an extract from a study conducted on Information Security Threats to eCitizen Services in Kenya. The research presents findings on information security measures to secure eCitizen services in Kenya. The case study adopted a descriptive research design that targeted 12,000 respondents (users) from 51 Huduma Centres countrywide. Purposive sampling was applied to select Huduma Centres and 10% of respondents from each centre. About 1,200 questionnaires were issued with a return rate of 966 responses at 80%. The study applied both quantitative and qualitative techniques in analysis. The hypothesis was tested at a 5% significance level. The study identified 10 categories of security measures, six of which are discussed in this paper i.e., National capabilities, institutional policies, capacity development, backups, physical access, professional certification, frequent ICT audits, firewalls and management security reviews. The study recommends locally modelled technological solutions, mutually beneficial cyber security collaboration, frequent infrastructure security audits, user capacity training and restructuring national security organs to create cyberspace manning capabilities. These sectoral changes will enhance preventive, defensive and offensive capabilities against arising cyberspace threats from geopolitical, technological, economic and security competition and rivalries among global nations, non-state actors and malicious individuals.

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

APA CITATION

Maina, L. W. & wa Otieno, G. O. (2024). Leveraging Technology for Government Service Delivery: Suggestions for Securing the eCitizen Services in Kenya. *East African Journal of Information Technology*, *7*(1), 81-91. https://doi.org/10.37284/eajit.7.1.1757

CHICAGO CITATION

Maina, Lucy W. and Godfred Ohndyl Otieno. 2024. "Leveraging Technology for Government Service Delivery: Suggestions for Securing the eCitizen Services in Kenya". *East African Journal of Information Technology* 7 (1), 81-91. https://doi.org/10.37284/eajit.7.1.1757.

HARVARD CITATION

Maina, L. W. & wa Otieno, G. O. (2024) "Leveraging Technology for Government Service Delivery: Suggestions for Securing the eCitizen Services in Kenya", *East African Journal of Information Technology*, 7(1), pp. 81-91. doi: 10.37284/eajit.7.1.1757.

IEEE CITATION

L. W. Maina & G. O. Otieno "Leveraging Technology for Government Service Delivery: Suggestions for Securing the eCitizen Services in Kenya", *EAJIT*, vol. 7, no. 1, pp. 81-91, Feb. 2024.

MLA CITATION

Maina, Lucy W. & Godfred Ohndyl Otieno "Leveraging Technology for Government Service Delivery: Suggestions for Securing the eCitizen Services in Kenya". *East African Journal of Education Studies*, Vol. 7, no. 1, Feb. 2024, pp. 81-91, doi:10.37284/eajit.7.1.1757.

INTRODUCTION

The 21st Century has witnessed technological transformations and the development of new digital solutions. 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, Amanda, & Sharp, 2018). 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, developing countries particularly in Sub-Saharan Africa (SSA) still lag due to poor economies, low penetration levels of technology, incapacities in education, high asset acquisition costs, lack of infrastructure and largely poor and illiterate populations. These poor performances also affect some countries in parts of Latin America and East Asia (Rose, 2019).

The UN through policy support initiatives has encouraged states to embrace digital economies. The 2020 UN E-Government Survey observes tremendous efforts by various governments in response to the influence of COVID-19 Pandemic that accelerated the implementation of e-governance programmes (UN E-Government Survey, 2020). 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 the UN SDGs.

At the local level, Kenya remains focused on enhancing the growth of digital knowledge-based economy. The Kenyan Constitution of 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 (Government of Kenya, 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 should speed up national transformations towards digital knowledge economy which is an important ingredient of Kenya's industrialization (Government of Kenya, Vision 2030).

The Kenya e-governance initiatives initially focused on; e-tax, e-customs, one-border stop, eCitizen, 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

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

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 bringing along ICT-based threats arising from global network connectivity (Ciampa, 2018).

The number of businesses that have experienced data breaches has grown exponentially during this 21st Century. The number of recorded cases and financial losses 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 overwhelmingly disastrous.

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 the opening of new cyber warfare domains and military defense restructuring capabilities to guarantee preventive, defensive and offensive capabilities within the cyberspace (Glikson & Anita, 2020). 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 (Shafqat & Ashraf, 2016). Additionally, 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 opportunities to intercept or steal institutional information and data for their unlawful use. This study thus sought to examine information security threats to e-government services in Kenya with the purpose of establishing potential security measures to secure the eCitizen services in Kenya for improved national digital economy and security as discussed.

RESEARCH METHODOLOGY

Research Design

The study used a descriptive research design in the collection, presentation and analysis of data in response to the problem of the study. The mixed method cross-sectional survey approach was further chosen. 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 conduction of final field questionnaire.

Target Population

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 service providers and users who sought Kenya government services from ten (10) service Centre/ categories purposively selected across the country out of the existing 51 Centres in Kenya including the foreign segment. The

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

study estimated at least 12,000 users of eCitizen service from 9 regions in Kenya and 1 segment representing foreigners (non-Kenyans). The 10 service centres under study were Embu Town, Garissa Town, Kakamega Town, Kisumu Town, Mombasa Town, Nyeri Town, Nairobi GPO, Nairobi, City Sq., Nakuru Town and Foreigners' service.

Study Sample and Sampling Techniques

The study adopted purposive and simple random sampling techniques. This is a procedure of selecting a subject to be included in a study by allocating equal chances to the elements in the population. (Creswel, 2007). The sampling frame was used by allocating numbers to potential respondents from the target population. The purposive sampling allowed the study to access respondents who 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).

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 was found to be suitable for this study because the researcher had the potential to reach a large number of respondents in a short period, 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 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.

Data Analysis and Presentation

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, and categorized using tables. The researcher used both quantitative (descriptives) and qualitative techniques (themes). The results were presented in tables, pie-charts, frequency and percentages. Content analysis was further used to process the qualitative data collected from the open-ended questions which were converted into quantitative data through the ordinal scale for ease of analysis and interpretation.

Ethical Considerations

The study strictly adhered to research ethical standards. 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.

RESULTS AND DISCUSSION

The target population of the study was 12,000 people and through purposive sampling, the study targeted a sample size of 10% of the population. 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%. A research response rate of 50% is considered adequate, rate of 60% is considered good and any rate above 70% is considered excellent (Kothari and 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 (Mugenda and Mugenda, 1999). Based on the

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

above assertions, the response rate of 80% returned by this study was thus found adequate to make credible deductions from the data collected and analysed by the study.

Table 3: Suggested measures for securing information security on the eCitizen platform

Preventive measures to information security threats	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly agree	Totals
National legislation on information & infrastructure security	62	31	71	337	465	966
Institutional policies, plans and strategies	57	18	75	309	507	966
Secure collaboration with service providers and application vendors/owners	53	44	84	238	547	966
National ICT Capacity Development & Innovations	49	13	89	242	572	966
National Technical Agency responsible for round-the-clock national cyberspace surveillance and monitoring	62	35	62	279	527	966
Professional training and certification of ICT operators	45	40	147	312	423	966
Enforce physical security, passwords and codes security control protocols for all users	61	9	92	250	553	966
Installation of ICT hardware power backup solutions	53	18	107	254	534	966
Frequent audits of ICT infrastructure, systems, procedures and regulations	53	31	71	245	565	966
Strategic-level national digital information security oversight & reviews	54	23	108	266	515	966
Sub Totals	**551**	**262**	**907**	**2731**	**5210**	**9660**

This table presents the summary of respondents who identified preventive measures against information security threats to the provision of eCitizen 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 indicate that 1719 respondents returned negative responses at 9% and 7941 respondents returned positive responses at 91%. This was an excellent response because any response above 70% is considered extremely good and excellent for decision-making (Kothari and Garg, 2014).

The identified measures are further discussed in the following section.

- **National Legislation and Institutional Policies**

The study found that 62 respondents Strongly Disagreed, 31 Disagreed, 71 Neither Agreed nor Disagreed, 337 Agreed and 467 Strongly Agreed. The study further made a finding that a summative 13% disagreed while 87% largely agreed that

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

national legislation is a prerequisite for establishing a secure policy environment for national digital information management. According to Tahira and Mugenda, any findings above 70% are considered excellent (Mugenda and Mugenda, 2003). A similar study by Sunil, Pawar and Bapu (2021), identified legislation, policies, rules, regulations and institutional procedures and processes as extremely important in enhancing system operations and safety against information security violations. The study thus deducts that national legislations, policies, rules and institutional regulations including protocols are necessary and important for enhancing system confidentiality, integrity, information safety, operational efficiency and liabilities from third-party stakeholders. The current legislations and policies enacted since 2014 are many and require harmonization with clear responsibilities among the agencies, the ministry, investors and service consumers. This will ensure that the eCitizen services are adequately founded on existing laws and policies and enhance security for both the nation and the public against exploitation and manipulation by foreign agents.

- **Secure collaboration and service contracting**

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 proper contracting and collaboration with third-party foreign contractors and owners of third-party licenses is essential to guarantee protection against security threats that face the eCitizen services delivery in Kenya. According to Tahira and Mugenda (2003), any findings above 70% are considered excellent. A similar study by Sunil, Pawar and Bapu (2021), found that foreign collaboration and proper contracting for the eCitizen services within established laws were extremely important in enhancing system efficiency and data security in the hands of third parties against security violations. Amorreti (2007), identifies that for an effective e-democracy and e-governance system, secure collaborations supported by appropriate policies are extremely essential and non-compromisable. The study thus deducts that strategic collaboration with contractors and third parties are important for protecting and securing quality service delivery, system confidentiality, integrity, information security, operational efficiency and third-party liabilities against the state and her citizens.

- **National ICT Capacity Development & Innovations**

The study found that 5% of the respondents Strongly Disagreed, 5% Disagreed, 9% Neither Agreed nor Disagreed, 25% Agreed and 56 % Strongly Agreed on the establishment of national capabilities. The study further made a finding that summative 19% disagreed while 81% largely agreed that in the 21st Century, nations require their own capabilities in ICT technological innovations. According to Tahira and Mugenda (2003), any findings above 70% are considered excellent. Irani et al (2007), observe that technical ICT skills are critical to bridge the digital divide in developing countries. The respondents observed that Kenya lacks its own capabilities and the entire private and public sectors have outsourced commercial third-party ICT technologies from foreign multinational corporations. Digital skills are essential for the design, implementation and management of the eCitizen platform and services. Development of relevant human capacities will facilitate effective management of the online services and maintenance of the systems, hence mandatory. Development of national capacity should be made a national priority by setting up renewed public-private sector-education ICT research and innovation centres to secure the nation in the fast-changing era of Artificial intelligence and the Internet of Things (IoT).

- **Setting up National Technical Agency**

The study found that 5% of the respondents Strongly Disagreed, 1% Disagreed, 9% Neither Agreed nor Disagreed, 25% Agreed and 60%

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

Strongly Agreed. The study further made a finding that summative 15% disagreed while 85% largely agreed that technical agency was a necessity to oversee the monitoring of the virtual space. According to Tahira and Mugenda (2003), any findings above 70% is considered excellent. Bacon et al (2007), observe that technical jurisprudence was not only essential but very important in protecting the national cyberspace. This was considered critical for guaranteeing national sovereignty and protection of national data against foreign espionage and malicious disruption of services. The study thus deducts that establishment of technical agency particularly within the national security architecture will be important towards securing the nation against foreign or third-party malicious agents. This however requires technically qualified staff backed with appropriate legislation and policy framework. This will build towards service stability, information integrity, safety, operational efficiency, consistency, reliability and against third-party liabilities.

- **Professional ICT Training and certifications**

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 professional ICT training and certification was a critical requirement to guarantee protection against information security threats that face the eCitizen services. According to Tahira and Mugenda (2003), any findings above 70% is considered excellent. Lopez (2002) 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-governance platforms and services. A similar study by Sunil, Pawar and Bapu (2007), identified professional training and certification as not only essential but very important in protecting system infrastructures and customer data and privacy. 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.

- **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 were important to guarantee protection against the information security threats that face the e-government services in Kenya. According to Tahira and Mugenda (2003), any findings above 70% is considered excellent. Camastra et al (2013) observe that installation of end-to-end backup security accompanied by physical equipment security, use of codes, authentic passwords and user protocols are not only essential but very important towards the protection of the system infrastructures and equipment integrity. 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.

- **Installations of ICT 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 backups are important protection and safeguards against the information security threats that face eCitizen services in Kenya. According to Tahira and Mugenda (2003), any findings above 70% is considered excellent. According to Bambang et al, (2017), it is very

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

important for the organizations with heavy investments in ICT digital systems and infrastructure to install operational backup support for essential hardware and software applications(Mirela, 2010). 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.

- **Frequent system and infrastructure audits**

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 eCitizen services in Kenya. According to Tahira and Mugenda (2003), any findings above 70% is considered excellent. According to Bambang et al (2017), 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 (Mirela, 2010). 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

- **Installations of firewalls and automated security 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 eCitizen services in Kenya. According to Mirella (2010), 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. 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. 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

- **Strategic level national digital 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 level information security reviews are important protection and safeguards against the information security threats that face e-governance services in Kenya. The management have the overall responsibility and accountable for the system security and safety of national data. As the policy makers this responsibility rests upon them. According to Mirella (2010), 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,

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

policies and procedures. The study thus deducts that top management information security reviews including parliamentary oversight are critical in the overall protection of national data, institutional ICT infrastructure, stability, integrity, information safety, operational efficiency, consistency, reliability and against third party intrusions. Strategic reviews will additionally provide confidence of investors in the ICT sector.

CONCLUSION AND RECOMMENDATIONS

As governments across the world continue to embrace e-governance in provision of public services and to significantly reduce bureaucracy, enhance efficiency, reduced corruption and fundamentally transform public service delivery, there is need to rethink and configure new technologically-driven service delivery avenues. Kenya has made great strides in improving access to public services by the citizenry, however threats of information leakage and misuse persist and may lead to service disruptions, subjugation of national security, loss of national independence and loss of national sovereignty. To overcome these contemporary global challenges, the study strongly recommends home-made technology solutions, nurturing local programming capabilities, strong policy measures, international collaboration with technology developers, frequent infrastructure security audits, employees and user capacity training, strategic reviews and upgrades in tandem to the evolving information security threats. Further research is recommended on the impact of information security threats on political elections, economic frauds, military operations and social communication. As the country migrates steadily into digital knowledge economy embracing integrated eCitizen public and commercial services there is need to create national cyberspace capabilities within the national security organs to provide for the preventive, defensive and offensive capabilities. These will be important towards guaranteeing national security and system infrastructure redundancy.

REFERENCES

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

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

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

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

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

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

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.

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

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

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage (2021). Cyber Crime, Cyber Space and Effects of Cyber Crime. Volume 7, Issue

Article DOI: https://doi.org/10.37284/eajit.7.1.1757

1 Page Number: 210-214 Publication Issue: January-February-

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

UN E-GOVERNMENT SURVEY (2020), publicadministration.un.org, Accessed on 20th August 2021 at 1246 pm

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

Wolf, Martin (2014) Shaping Globalisation. Washington DC: International Monetary Fund, Accessed on 20 August 2022, 51

