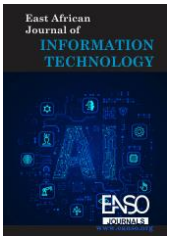

East African Journal of Information Technology
eajit.eanso.org
Volume 7, Issue 1, 2024
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Leveraging Technology for Government Service Delivery: Suggestions for Securing the e-Citizen Service 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:

Information Security, e-Citizen, e-Governance, Service Delivery.

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 and non-state actors, mostly multinational corporations (MNCs), have equally exposed user governments, such as Kenya, to significant cyberspace security threats, service disruptions and exposed national security leading to interferences in national autonomy and at times threatened national sovereignty. The threats arise from the activities of offensive states, malicious non-state actors 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 e-Citizen services in Kenya. The research presents findings on the effectiveness of information security measures initiated to secure the e-Citizen services in Kenya. The case study adopted a mixed method design combining cross-sectional and descriptive research design that targeted 12,000 respondents (users) from 51 *Huduma* Centres countrywide. Purposive sampling was applied to select 10 *Huduma* centres and 10% of respondents from each of the selected centres. About 1,200 questionnaires were issued with a return rate of 80% which translates to 966 responses. The study applied both quantitative and qualitative techniques in analysis. The study identified 10 categories of security measures which are discussed in this paper categorized under legislation and policy; infrastructure and capacity development; protective action; monitoring and oversight. From the findings, Kenya has implemented the measures of information security to a satisfactory level even though more is needed in terms of engaging the populace to enhance safe data use, handling and storage. In order to bolster a safe service delivery e-Citizen system, the study recommends locally modelled technological solutions, mutually beneficial cyber security collaborations, 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 e-Citizen Service 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 e-Citizen Service 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 e-Citizen Service 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 e-Citizen Service 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 e-Citizen Service 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 vast 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 revolutionized modernization and thus globalisation of the world production, manufacturing, service, markets and public organization (Kremling, & Parker, 2018). Advanced countries have continued to take the 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 the Sub-Saharan Africa (SSA) still lag behind due to poor economies, low penetration levels of technology, incapacities in technical skills, high asset acquisition costs, lack of infrastructure and largely poor and low-educated populations. These realities are replicated in poorly performing countries in parts of Latin America and East Asia (Farina, 2019).

Global organizations such as the UN continue to encourage states to embrace digital economies through policy support initiatives. The 2020 UN e-Government Survey for instance observes tremendous efforts by various governments in response to the effects of the 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 including the adoption of technologies that support remote provision of services. This African Agenda 2063 initiative largely mirrors the UN SDGs and acknowledges the central role of digital technologies in fast-tracking the achievement of the goals (AU, 2015).

At the local level, Kenya remains focused on enhancing the growth of a 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 (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 are expected to catalyze national transformations towards a digital knowledge economy which is an important ingredient of Kenya's industrialization framework (Government of Kenya, Vision 2030).

In Kenya, the right to information security and privacy are underpinned in the Constitution of

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

Kenya, Article 31 (c), which guarantees every person the right to privacy of information relating to family or private affairs. From this supreme law springs other sets of legislation and policies protecting private information such as that used and shared through the e-Citizen government service platform. The most elaborate and relevant law is the recently enacted Data Protection General Regulations of 2021 which are sets of laws requiring data controllers and processors to protect and hold in privacy all information regarding citizens that they serve. It also defines the procedures for enforcing the rights of data subjects and the duties and obligations of such data handlers. Under these laws, it is illegal and punishable to share or expose personal information shared by clients for other purposes other than service use. Earlier in 1998, the Kenya Information and Communication Act was the overarching law that controlled the use and access to information and communication technologies in Kenya. This law contains the requirements and compliance standards that govern service providers who have client's data in their custody. Additionally, sector-specific data regulations exist such as the National Payment System Act of 2011 which regulates how personal data is handled in payment systems. Banking systems are regulated by the Prudential Guidelines for Institutions Licensed Under the Banking Act which obligates banks to protect and safeguard customer data. Additionally, the National ICT Policy Guidelines of 2020 have provided a framework for advancing modern technologies in an orderly manner cognizant of individuals' right to privacy while designating how personal data can be used, distributed, analysed, enhanced and converted for other uses. Other laws regulating the use of cyberspace are contained in various legislation such as the Computer Misuse and Cybercrimes Act, No. 5 of 2018, which defines and criminalizes offensive acts on the cyberspace as cybercrime offences; the Kenya Information and Communications (Consumer Protection) Regulations (2010) whose aim is to protect consumers of ICT services and products; Guidelines on Cybersecurity for Payment Service Providers, of 2019 whose aim is to provide a secure cyberspace and combat cybercrime.

The Kenya e-governance initiative initially focused on e-tax, e-customs, one-border stop, e-Citizen, e-passport, e-cities, e-health, among many other public services offered within central government and County devolved units. For effective penetration and easy access to public service by the citizenry, 53 *Huduma* Centres have been established since 2014 in major towns across the 47 Counties of Kenya. Operating as one-stop service platforms, *Huduma* Centres are anchored upon the notion of *Whole of Government* approach and have become centres where services of Ministries, Departments, Agencies and County governments (MDACs) are deployed in an integrated and coordinated manner. Alongside the centres, 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, as well as infrastructure expansion and internet connectivity (KNBS, 2022). These successes are however happening within a globalizing world attracting cyber security threats within the largely declining national sovereignty environment bringing to the fore ICT-based threats arising from the global network connectivity (Ciampa, 2018).

The number of businesses that have experienced data breaches globally and regionally continues to grow exponentially during this 21st Century. Consequently, 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 customers and applicant

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

accounts in March 2019 (Clement, 2019) posing one of the largest credit card scams ever known. For a government, the cost of data breaches can be overwhelmingly disastrous. Kenya as a country has not been spared either and in 2023, the country's e-Citizen platform and other critical infrastructure faced a Distributed Denial-of-Service (DDoS) cyber-attack that left the systems inaccessible bringing to the fore the potential for severe security, reputational and economic implications of cyber-attack to the nation and affecting the continuing digitization of government services.

According to Libicki (2012), cyberspace has become the next frontier of war and nations are constantly under threat due to its interconnected and interdependent structure. The growth and proliferation of Artificial Intelligence (AI) 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 defence restructuring capabilities to guarantee preventive, defensive and offensive capabilities within the cyberspace (Glikson, & Woolley, 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, & Masood, 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 a greater opportunity to intercept or steal the institutional information and data for their own unlawful use. Given this scenario, this study thus sought to examine information security threats to e-government services in Kenya with the purpose of establishing the efficacy of security measures instituted to secure the e-Citizen service in Kenya for improved digital economy and national security.

RESEARCH METHODOLOGY

Research Design

The mixed method approach applying both quantitative and qualitative techniques was adopted for the study. A cross-sectional survey design allowed the analysis of data from different study sites at a single point in time. The method was deemed reliable for the collection of data from the target population of users drawn from various *Huduma* Service Centres in Kenya and in analysing the e-Citizen services provided, the information security threats, the consequences of information security threats and the preventive measures against information security threats to the e-government service. Qualitative approach was used to gather data from persons responsible and accountable for systems and services at the *Huduma* centres such as the unit and line managers as well as the supervisors of different processes and especially data handling at the centres. Before the commencement of the actual study, a pilot survey was conducted at the Kiambu town *Huduma* centre that allowed pretesting and correction of the instruments that were used to conduct the field study. Reliability of the main instrument was found satisfactory at 0.7 Cronbach Alpha.

Target Population and Sampling Technique

The population for this study was drawn from users and service providers of Kenya's e-Citizen government service from the 51 active *Huduma Centres* targeting both Kenyans and foreigners. In sample selection, the study adopted purposive and simple random sampling techniques. Purposive sampling allows the selection of respondents with the required information with respect to the objectives of the study (Creswell, & Creswell, 2017). Out of 51 centres, 10 service centres were purposely selected taking care to include urbanized, rural, frontier counties and 1 centre dedicated to serving foreign residents in Kenya. The 10 service centres selected were: Embu Town, Garissa Town, Kakamega Town, Kisumu

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

City, Mombasa City, Nyeri Town, Nairobi GPO, Nairobi, City Sq., Nakuru Town and foreigners' service which mainly provided immigration and work permit renewals. The study estimated at least 12,000 users of e-Citizen service from the 9 regions in Kenya and 1 segment representing foreigners (non-Kenyans). The sample size of 10 % was considered sufficient and representative for analysis (Mugenda, & Mugenda, 2003) leading to the selection of 1,200 users for the study.

Data Collection Instrument

A structured questionnaire was self-administered and filled out by the user respondents and contained both closed and open-ended questions for the respondents to record their answers. The instrument was preferred since it had the potential to reach a large number of respondents in a short period of time, provide respondents with adequate time to respond, afforded anonymity and objectivity since the instrument does not result in biases of personal characteristics (Creswell, 2016). The research questionnaire was organized according to the major objectives of the study and comprised four sections covering demographic information, e-government services utilized, information security threats and perceptions on the preventive measures in place to safeguard information security threats against the e-governance platform. Additionally, a key informant interview guide was utilized to collect data from *Huduma* centre supervisors, unit and line managers as well as ICT staff within the establishments.

Data Analysis and Presentation

The completed study questionnaires which were received back from the respondents were sorted and checked for errors, omissions and biases. Quantitative data was further coded and processed using descriptives while qualitative data was sorted, classified and categorized using content analysis procedure and presented thematically.

Ethical Considerations

The study strictly adhered to research ethical standards. The questionnaire was explicit and gave complete assurance of the respondents' confidentiality, anonymity, privacy of information provided as well as voluntary participation in the study. After collection, the questionnaires were anonymized by removing all identifiers which were replaced with regional codes known only to the researcher. Additionally, the researcher upheld the highest level of integrity in the collection of the data and adhered to all the statutory requirements and policy guidelines for research in Kenya.

Results and Discussion

A total of 1,200 questionnaires were sent out to the potential respondents in the 10 regions identified by the study. From the 1,200-target sample, 966 respondents filled and returned the questionnaires making a response rate of 80%. The research response rate of 50% is considered adequate, a 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 (Hira, & Mugenda, 1999). Based on the 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. From the findings, respondents sought various government services on the e-government platform which were classified as government to citizen (G2C) inclusive of civil registrations, property and general services; government to business (G2B) inclusive of licenses, revenues, taxations and permits; government to government (G2G) such as private and commercial services; and government to employees (G2E) services inclusive of salaries, reports, instructions and making returns.

The core objective of this paper was to establish if security measures for protecting personal information and data were adequate. Thus, the study sought to find out from users and those in charge of *Huduma* centres if the measures taken to secure user information were considered

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

adequate. These measures were grouped into 4 tracks: legislation and policy; infrastructure and capacity development; protective action; monitoring and oversight. The respondents were asked to indicate their level of agreement on whether the measures in place were adequate using a 5-pointer Likert scale as captured in Table 1. From the table, the findings are generally in agreement that the measures that are in place to counter possible threats to user information were adequate. About 5,208 responses across the different measures under investigation indicate a strong agreement with the statement, 2732 responses indicated concurrence while 906 were neutral. On the other hand, a total of 262 responses were in disagreement and 549 strongly disagreed that the various security-enhancing measures in place were adequate. The findings are further elaborated in the next section.

Table 1: Opinion on measures for securing information security on the e-Citizen platform

The following measures against information security threats are adequate	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly agree	Totals
National legislations 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
Enforcement of physical security, passwords and code security control protocols for all users	61	9	92	250	553	966
Installation of ICT hardware power backups 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
Total responses	**559**	**262**	**906**	**2732**	**5208**	**9660**

- ***National Legislation and Institutional Policies***

Studies affirm that national legislation is a prerequisite for establishing a secure policy environment for national digital information management. For instance, Pawar, Mente and Chendage (2021), identified legislation, policies, rules, regulations and institutional procedures and processes as extremely important towards enhancing system operations and safety against information security violations. The study found that 62 (6%) respondents strongly disagreed, 31 (3%) disagreed, 71 (8%) neither agreed nor disagreed, 337 (34%) agreed and 465 (48%) strongly agreed that the legislations and policies were adequate. Overwhelmingly, 82% expressed confidence in national legislation and policy to safeguard their information. Further, findings from key respondents in this study among them the service providers and supervisors indicated that while national legislation covers information security adequately, there is need for a much deeper engagement and discussion with the public

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

to enhance an appreciation of existing laws and individual responsibility such as that pertaining to protecting one's log-in credentials and passwords. Further views from key informants were that there were too many laws currently which were confusing. The study thus deducts that the evolving national legislations, policies, rules and institutional regulations including information access protocols are timely and key towards enhancing people's confidentiality in system integrity, information safety, operational efficiency and liabilities from third-party stakeholders. However, 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 e-Citizen services are adequately founded on existing laws and policies and enhance security for both the nation and the public against exploitation and manipulation by malicious local or foreign agents.

- ***Institutional policies, plans and strategies***

The study sought to find out if institutional policies and strategies were enough to safeguard user information. From Table 1, 507 (52%) expressed strong agreement, 309 (31%) agreed, 75 (8%) were neutral while 18 (2%) disagreed and 57 (9(%) strongly disagreed. The confidence expressed by the respondents in this area may be interpreted to mean that key players have properly operationalized the governing laws and have elected the right strategies to safeguard user information. Findings from the key informants echoed the same findings with most indicating that government and key players were continuously pursuing user information security as a goal. There was a general agreement among key informants that security breaches were taken seriously and acted upon promptly by concerned departments. These findings are indicative that the country's policy and planning landscape in place are supportive and configured towards ensuring user information security.

- ***Secure collaboration and service contracting***

The nature of e-government service delivery is that a lot of information is shared and used by different users. The study sought to find out if there existed secure collaborations among information users and if these were anchored on service contracting. The study found that a majority 547 (56%) strongly agreed while 238 (24%) agreed that these were adequate while 84 (9%) remained neutral. 53 (5%) of the respondents strongly disagreed and 44 (5%) disagreed that there were secure collaborations and contracts. Findings from key informants interviewed in the study indicated that third-party foreign contractors and owners of third-party licenses were thoroughly securitized and vetted to guarantee protection against security threats that face the e-government services delivery in Kenya. Pawar, Mente and Chendage (2021) have observed that foreign collaboration and proper contracting for e-government services within established law was extremely important towards enhancing system efficiency and data security in the hands of third parties against security violations. Amoretti (2007) further posits that for an effective e-democracy and e-governance system, secure collaboration supported by appropriate policies are extremely essential and should never be negotiated. The study thus deducts that strategic collaboration with contractors and third parties are important and have been activated 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 and Innovations***

Regarding the capabilities of the national ICT system and innovations for securing the e-government service delivery, the study found that only 49 (5%) of the respondents strongly disagreed while 13 (1%) disagreed that these were adequate. Conversely, 242 (25%) agreed and 572 (59%) strongly agreed that these were strong enough. Key informants further affirmed that the

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

national ICT landscape was fast changing in response to global trends and that Kenya was on the right track in maintaining the ICT innovation lead in the region. The interviewed respondents further 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 implying that Kenya needs to fast-track the development of its own homegrown solutions. Some respondents felt that the slow take-off of the much-anticipated "Kenyan Silicon Valley" situated at Konza City was taking too long further jeopardizing digital space security. Irani et al. (2007) observe that technical 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-Citizen platform and services. Development of relevant human capacities will facilitate effective management of the online services and maintenance of the systems and are therefore mandatory. Thus, the study infers that the development of national capacity should be made a national priority by setting up public-private sector-education, ICT research and innovation centres to secure the nation in the fast-changing era of digital innovations.

- ***Setting up National Technical Agency***

Respondents were asked to indicate if the Kenya government had a reliable national technical agency responsible for round-the-clock national cyberspace surveillance and monitoring. The study found that 527 (54%) strongly agreed with the statement while 279 (28%) agreed. 62 (6%) of the respondents strongly disagreed, 35 (3%) disagreed while 62 (6%) neither agreed nor disagreed. Bacon *et al*. (2007) observe that technical jurisprudence was not only essential but very important towards protecting the national cyberspace. Findings from key informants in the study on the technical body mandated to audit and monitor the e-government systems were mixed with most citing the Communication Authority of Kenya as the legal technical agency. Others were of the view that more than one agency were responsible citing among others the National Computer and Cybercrimes Coordination Committee and the Kenya Computer Incident Response Team Coordination Centre. A few of the key informants expressed uncertainty on whether any of the agencies in place were 'hands-on' implying that they were not actively involved in closely monitoring information threats. Further, key informants indicated that the technical agencies are critical towards guaranteeing national sovereignty and protection of national data against foreign espionage and malicious disruption of services. The study thus deducts that the establishment of a 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 Certification of ICT Operators***

López (2002) observes that ICT skills are critical to bridge the digital divide in developing countries. The study sought to establish the adequacy of professional ICT training and found that 312 (32%) agreed and 423 (43%) strongly agreed that it was sufficient. About 5% (45) of the respondents strongly disagreed while 40 (4%) disagreed with the assertion with 15% opting to remain neutral. Key informants in the study concurred that professional ICT training and certification was a critical requirement to guarantee protection against information security threats that face the e-Citizen services. They further affirmed that digital skills are essential for the design, implementation and management of the e-governance platforms and services. Asked if Kenya had enough qualified and certified ICT personnel, most key informants were affirmative but cited an imbalance in posting such personnel in the public service citing that private enterprises were at an advantage in attracting such workers due to higher salaries. A few of the informants

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

expressed that more focused training in defensive strategies was required to secure user information, particularly in the e-government system. Other studies (see Farina, 2019; Sunil, et al., 2021; Khisa et al., 2020; Pawar & Bapu, 2007), identified professional training and certification as not only essential but very important towards protecting system infrastructures and customer data and privacy.

- ***Physical Security, Codes, Passwords and Control Protocols***

To establish the status of preventive measures used in securing information, the study sought from respondents their views on the adequacy of physical security measures such as passwords and access code protocols. From the study 553 (57%) strongly agreed while 250 (26%) agreed that the access protocols were adequate. About 61 (6%) of the respondents strongly disagreed with 9 (1%) disagreeing with the statement while 92 (10%) were neutral. Camastra et al. (2013) observe that installation of end-to-end backup security accompanied by physical equipment security, use of codes, authentication passwords and user protocols are not only essential but very important towards the protection of system infrastructures and equipment integrity. Key informants in the study concurred that the digital platform was well guarded through limits of access and complex user protocols that were closely manned and monitored internally. They also affirmed that user passwords were highly controlled and changed frequently and attempted internal breaches were expeditiously dealt with. The study thus deducts that physical security, use of codes, authentic passwords and user protocols are considered as well implemented across the e-government service for 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***

To ascertain the perceived status of ICT hardware and software backups that allow the recovery of lost information in case of breach, the study sought to find out from respondents if these were found adequate. A majority 534 (55%) of the respondents strongly agreed, 254 (26%) agreed, 53 (5%) strongly disagreed while a paltry 18 (1%) of the respondents disagreed with 107 (11%) remaining non-committal. Sutopo et al. (2017) and Gheorghe (2010) emphasize the importance of installing operational backup support for essential hardware and software applications for organizations with heavy investments in ICT digital systems and infrastructure. Most key informants in the study voiced their concern with the available backup system observing that they could not be relied upon should the e-government platforms collapse over malicious activity. They observed that the government and stakeholders were reluctant to invest in elaborate backup options. This finding may be a pointer to a situation of system vulnerability and an indication that massive data could be lost in case of a severe cyber-attack.

- ***Frequent System and Infrastructure Audits***

Frequent audits of ICT systems, infrastructure and procedures is an important function to guarantee the institutional protection against information security threats. Gheorghe (2010) further observes five important dimensions of the e-government functions whose audit remains important including policy, institution, infrastructures, applications and planning. Undertaking an audit of the entire system infrastructure and procedures once implemented helps determine the efficiency levels and effectiveness of the investment. In the study, an overwhelming majority 565 (58%) perceived adequate the system and infrastructure audits currently in place. A further 245 (25%) found them adequate while 53 (5%) strongly disagreed and a further 31 (3%) disagreed. About 71 (7%) were neutral choosing neither to agree or disagree. Key informants interviewed in the study reported that auditing was a frequent practice and that periodic reporting on system failures and faults were a requirement. The findings are indicative that preventive action was being undertaken to secure the e-government platforms.

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

- ***Strategic Level National Digital Information Security Reviews***

The management of any organization bears the overall responsibility and is accountable for system security and safety of national data. To gauge if the e-government services were closely monitored by persons of responsibility at the national strategic levels, respondents were asked to indicate if the strategic level system review were adequate. 515 (53%) strongly agreed while 266 (28%) agreed they were adequate. On the other hand, 54 (6%) of the respondents strongly disagreed and 23 (2%) disagreed with 108 (11%) remaining neutral. Key respondents opined that monitoring and reviews are the responsibilities of policymakers who must be accountable to the citizenry as far as the use and handling of their personal data is concerned. Some key informants expressed that the government through law has assured the public of the safety of their data and that required periodic updating of the security of information. However, a few key informants expressed that data accountability by government and collaborating agencies was not properly enforced and much more improvement was required in this area. According to Gheorghe (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, policies and procedures. Strategic reviews and updates will additionally provide confidence to investors in the ICT sector.

CONCLUSION AND RECOMMENDATIONS

As governments across the world continue to embrace e-governance in the provision of public services and to significantly reduce bureaucracy, enhance efficiency, reduce corruption and fundamentally transform public service delivery, there is need to rethink information security and especially the use, access, retrieval and analysis of personal data acquired during service provision. Kenya has made great strides in improving access to public services by the citizenry through digital platforms. The study has established the adequacy of preventive and protective measures that are in place to counter information threats across the domains of legislation and policy, infrastructure and capacity development, protective action, monitoring and oversight. However, in cognizance that threats of information security and misuse persist and are fast morphing, there is need for more stringent frameworks to especially bridge gaps in training and capacity, citizens'/user engagement, monitoring and auditing which emerge from this study. To overcome the contemporary global challenges to information security, 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. As the country migrates steadily into digital knowledge economy embracing integrated e-Citizen 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 sovereignty. Lastly, further research is recommended on the impact of information security threats on political elections, economic frauds, military operations and social media communication.

REFERENCES

Amoretti, F. (2007). ICTs Policies: E-Democracy andE-Government for Political Development.

AU Agenda 2063. (2015). Retrieved from https://au.int/en/agenda2063/overview (Accessed August 20, 2021, 12:46 PM).

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

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

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

Ciampa, M. (2009). *Security awareness: Applying practical security in your world*. Course Technology Press.

Clement, J. (2019). Number of internet users worldwide from 2005 to 2018 (in millions). *online: https://www. statista. com/statistics/273 018/number-of-internet-users-worldwide, retrieved on= October*.

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

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

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

Gheorghe, M. (2010). Audit Methodology for IT Governance. Informatica Economica, 14(1).

Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, *14*(2), 627-660.

Government of Kenya. (2010). The Constitution, 2010. Retrieved from http://kenyalaw.org/kl/in dex.php?id=398 (Accessed August 14, 2022, 11:30 PM).

Government of Kenya. (2015). Vision 2030. Retrieved from https://vision2030.go.ke/ (Accessed August 20, 2021, 12:46 PM).

Government of Kenya. (2019). The Data Protection Act. Retrieved from http://www.kenyalaw.org

Government of Kenya. (2021). The Data Protection (General) Regulations, 2021. Kenya Gazette Supplement No. 236. Retrieved from https://www.odpc.go.ke/wp-content/uploads/2021/06/L.N

Government of Kenya. (2008). Vision 2030. Government Printer.

Hira, T. K., & Mugenda, O. M. (1999). The relationships between self-worth and financial beliefs, behavior, and satisfaction. *Journal of family and consumer sciences*, *91*(4), 76.

Irani, Z., Love, P. E., & Montazemi, A. (2007). E-government: past, present and future. *European Journal of Information Systems*, *16*(2), 103-105.

Kremling, J., & Parker, A. M. S. (2017). *Cyberspace, cybersecurity, and cybercrime*. Sage Publications.

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

Kenya National Bureau of Statistics (2022). Economic Survey 2022. Retrieved from https://www.knbs.or.ke/wp- content/uploads/20 22/05/2022-Economic-Survey1.pdf

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

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

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *Isjlp*, *8*, 321.

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

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative & qualitative apporaches* (Vol. 2, No. 2). Nairobi: Acts press.

Pawar, S. C., Mente, R. S., & Chendage, B. D. (2021). Cyber crime, cyber space and effects of cyber crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(1), 210-214.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129-136.

Sutopo, B., Wulandari, T. R., Adiati, A. K., & Saputra, D. A. (2017). E-government, audit opinion, and performance of local government administration in Indonesia. *Australasian Accounting, Business and Finance Journal*, *11*(4), 6-22.

UN Department of Economic and Social Affairs. (2020). UN e-Government Survey. Retrieved from http://publicadministration.un.org (Accessed August 20, 2021, 12:46 PM).

