REVIEWED JOURNAL INTERNATIONAL of BUSINESS MANAGEMENT
ISSN 2663-127X

Vol. 4, Iss. 1 (2023), pp 471 – 477, October 27, 2023. www.reviewedjournals.com, ©Reviewed Journals

AN EXAMINATION OF THE EFFECTS OF CYBER SECURITY IN ENHANCING PERFORMANCE OF THE PUBLIC SECTOR INSTITUTIONS: LITERATURE REVIEW

[1] William Kiplimo Too & [2] Dr. Morrison Mutuku, PhD

[1] PhD Candidate, Kenyatta University, Kenya
[2] Lecturer, Management Science Department, Kenyatta Univeristy, Kenya

Accepted: October 7, 2023

ABSTRACT

The anticipated outcomes of this study was to gain a deeper understanding of the current state of cyber security adoption by the public sector institutions, especially in Kenya. The study reviewed on different literature on the status of cyber security adoption in regard to the enhancement on the performance of these institutions, identified challenges that the institutions faced in adopting and implementing such cyber security technologies, and the strategies needed to improve on cyber security applications. The review also pointed out cyber security measures that can lead to improved service delivery, increased operational efficiency, and more secure digital environment for the country's citizens. Thus, by identifying the challenges and barriers faced by these institutions, the study could help inform policy and decision-making processes, guiding future investments in cyber security and other related technologies. Further, the findings of this research could contribute to the enhancement of cyber security measures and their implementation in Kenya's public sector institutions. This, in turn, could lead to improved service delivery, increased operational efficiency, and a more secure digital environment for the country's citizens. By identifying the challenges and barriers faced by these institutions, the study could also help inform policy and decision-making processes, guiding future investments in cyber security technologies.

Keywords: *Cyber Security, Artificial Intelligence, Security Challenges, Security Measures, Digital Environment*

CITATION: Too, W. K., & Mutuku, M. (2023). An examination of the effects of cyber security in enhancing performance of the public sector institutions: literature review. *Reviewed Journal International of Business Management*, 4 (1), 471 – 477.

INTRODUCTION

Organizations should prioritize security and take precautions to reduce risks in order to guarantee the security of their information systems. Establishing robust access control methods that include authentication and authorization processes is a key first step. While authorization determines a user's level of resource access, authentication verifies a user's identity. This limits access to authorized individuals and helps prevent unauthorized access to confidential information. Encrypting sensitive data both in transit and at rest is a crucial additional precaution (Olayemi, 2014).

To prevent unwanted access, data is encrypted by being transformed into code. This makes sure that even if hackers get the data, they are unable to interpret it. To find system vulnerabilities and fix them right away, regular security audits and assessments are needed. By doing this, the system is guaranteed to be secure and resistant to potential threats. It's also crucial to educate staff members on cybersecurity and the dangers of accessing or sharing sensitive data. This includes instruction on the use of strong passwords, safe web browsing practices, and avoiding phishing schemes (Norris and Moon, 2015)

In conclusion, information system security is crucial, especially for online banking and e-government services. In order to reduce risks and ensure the confidentiality, integrity, and accessibility of sensitive information, organizations should prioritize cyber security and put the required safeguards in place.

Cyber Security

The techniques and strategies used to defend cyberspace against many types of known and unknowable threats are referred to as cybersecurity. In order to protect information systems, companies, and their assets, the International Telecommunication Union defines cybersecurity as a combination of measures including security strategies, threat management, engagement, training, best practices, and expertise. (International Telecommunication Union, 2018). Information and communication technology (ICT) can be a target or a tool in cyberattacks conducted by bad actors. Cybersecurity is essential to preventing such assaults on the internet, computer networks, electrical systems, and other devices (Olayemi, 2019).

Businesses rely heavily on the internet in the information age, making cybersecurity even more important. Hacking and data breaches may expose private information, which would hurt an organization's ability to compete. (Tarimo, 2016). Successful cyberattacks can jeopardize the confidentiality, integrity, and availability of an organization's ICT systems as well as the data they contain. (Bulgurcu et al., 2020). Cyber theft, often known as cyber espionage, exposes financial, proprietary, or secret information, providing the intruder an edge while costing the legitimate business money or intellectual property.

Public Sector Institutions in Kenya

Offices in the National Government, County Governments, and other independent institutions are considered public offices if their salaries and perks are paid from the Consolidated Fund or resources allocated by the Kenyan legislature. On the other hand, public services are those that are offered by the government to those who reside within its borders, either directly through the public sector or by subsidizing service delivery. Various government agencies offer these services as part of completing their particular missions. Public institutions are increasingly interacting with and serving their users through ICT infrastructure.

The National Government is primarily run by Ministries and parastatals, which are created by executive order by the President. The National Government now consists of twenty (20) Ministries, each of which is led by a Cabinet Secretary and supported by a Principal Secretary, a team of technical personnel, and a Principal Secretary. According to Article 226(3) of the 2010 Constitution of Kenya, while the ministries and respective state departments carry out their mandate through established teams of respective core and support functions technical teams, the processes, controls, and risk management are subject to review by the Auditor General. Ministries are also subject to assessment by internal auditors who, ideally before external audit review, provide management with advice on risk exposure and suggest corrective measures.

Even though certain engagements for external audits include the obligation to evaluate security, this is often not one of the tasks for the audits of final financial accounts. Internal auditors are a trustworthy source of cybersecurity information for ministries because the internal audit IT audit role frequently includes the duty to analyze cybersecurity.

Statement of the Problem

E-government solutions are created to conveniently and constantly deliver governmental services across open and distributed networks. Both the public and commercial sectors must ensure the security and dependability of information transferred through these networks, while they may place different priorities on security. The social characteristics of the nation in which they are implemented have an impact on a variety of aspects, including personnel, infrastructure, processes, and technologies that are essential to the success of e-government systems (Norris and Moon, 2015)

According to cyberattacks that attacked government websites in 2014 that contained financial, security, and state secret information, Kenya's public sector, which includes government ministries and related parastatals, is most at danger for such assaults. In addition to the recovery costs, these attacks spread panic and caused losses of more than Ksh5 billion. By undermining stakeholders' trust in e-government programs, such assaults impede the provision of public sector services. Therefore, research into the variables that influence cyber security in public services is necessary (Dhillon and Torkzadeh, 2016)

Previous studies have emphasized the connection between organizational management, security issues, and e-government. (Backhouse, 2021). The majority of research has been on technical problems, quantitatively examining information system security. (Siponen and Oinas-Kukkonen, 2017). But an objective assessment of information system security emphasizes the significance of non-technical problems in addition to technical ones for protecting sensitive information (Dhillon and Torkzadeh, 2016; Siponen and Oinas-Kukkonen, 2017). Prior research has mostly been done in wealthy nations, thus there isn't much literature covering the environment, population awareness, sociocultural dynamics, and how these factors affect conventional approaches to information system management in developing nations.

Since public and private organizations function differently, each requires specific management techniques. (Caudle, 2021; Fryer, 2017; Joia, 2023; Moon, 2020). The allocation of funds by public bodies' executive and legislative branches must be the subject of open conversations and strategic planning, which can have a political impact. In addition, regardless of their economic justification, public institutions must be geographically distributed and produce goods for the benefit of the public rather than for financial viability. Accordingly, managing public entities demands adherence to their unique procedures and security frameworks. (Wimmer and von Bredow, 2021). E-government systems present privacy and security issues due to the openness, dissemination, and availability requirements. (Norris and Moon, 2015; Ebrahim and Irani, 2015). With only a few empirical studies on the topic, the literature implies that there is a dearth of study on ICT, particularly e-government, and cyber security in developing nations. Wechuli (2014) evaluated the cyber security assessment framework used by Kenyan government ministries, looking at the strategies, baseline assessments, and asset prioritization that restrict the system's efficacy.

This study is comparable to the suggested research, which would assess cyber security in the public sector with an emphasis on leadership and human aspects that affect the framework's application. Wekundah (2015) looked into how cybercrime affected SMEs in Kenya and discovered that the majority of them did not prioritize cybercrime prevention or had the skills and experience required to address cyberattacks.

Study by Nyawanga's (2015) who researched on cyber threats in the Kenyan banking industry discovered that rates of cybercrime had drastically increased in the previous year, with the majority of attacks coming from China and Kenya, and that many bank workers were participating in cybercrime. This study will delve deeper into the organizational and human factors that influence cyber security in Kenyan National Government

Ministries, which have been repeatedly targeted by cyberattacks despite having a framework in place. Previous research has focused on different contexts, such as the private or public sectors.

Research Objectives

This study established the effect of cybersecurity enhancement on performance of the public sector institutions in Kenya. The objectives included, to investigate the level of cyber security adoption in public sector institutions in Kenya; to determine the effect of cyber security enhancement on the performance of public sector institutions in Kenya; to evaluate the challenges that public sector institutions in Kenya face in adopting and implementing cybersecurity and artificial intelligence; and to recommend strategies for improving the adoption and implementation of cybersecurity and artificial intelligence in public sector institutions in Kenya.

LITERATURE REVIEW

Empirical Review

The different organizational and psychological elements that influence computer and information security have been the subject of several studies (CIS). These studies have looked at issues such management support for CIS adoption and implementation, employee acceptance and adherence to security policies, and the adoption and implementation of security strategies and policies (Nyawanga's 2015). These studies have also uncovered a number of cultural components of security systems, including trustworthy security procedures, governance, coordination, and control, support from top management, employee involvement and training, and employees' enjoyment of security. Other studies have looked into how organizational and human characteristics affect information system security (Wimmer and Bredow, 2021).

Ibikunle and Eweniyi (2013) identified a number of goals for cyber-security in Nigeria, including addressing flaws in ICT systems and networks, fostering a culture of cyber security in institutions and people, promoting efficient collaboration in cyber security between private and public organizations, staying current with developments in cybercrime and their solutions, and ensuring the accessibility, confidentiality, integrity, and authenticity of systems.

In their survey on cloud computing security issues and solutions, Hussein and Khalid (2016) proposed a three-layered model for cloud computing security, with the first layer consisting of appropriate authentication methods for user identification, the second layer including data identification and encryption for security, and the third layer including the use of cryptography methods to secure data transmission. Deshpande and Sambhe (2020) examined the most recent cyber security concerns in India and discovered that while users prioritize security for personal computers, they frequently overlook protection for mobile devices, despite the fact that these devices might also be the target of cyberattacks. According to the report, personal firewalls can shield certain devices from threats that originate via the internet or the "air connection."

In their analysis of the literature, Deore and Waghmare (2016) concluded that the majority of public and commercial institutions are attempting to safeguard data and information from cyberterrorists or hackers. The authors point out that sharing data is a problem for both public and private companies, and a number of strategies are being created to safeguard data from hackers. In his study on the security of e-government systems in developing nations, Alfawaz (2018) identified a number of critical elements that have an impact on e-government security, including top management support, staff and management security awareness, information system security infrastructure, security culture, management style, management change and security, and privacy regulations.

Information security is constrained not only by technological advancements but also by political, cultural, legal, and moral behaviors of society, according to Kyobe's (2018) research on information security issues and their implications for developing e-government structures in some African countries. According to the study, security issues are made more difficult and delicate by the fact that e-government operations include a large number of citizens and are constrained by numerous legal frameworks and regulations. Wechuli (2014) examined strategy, baseline assessment, priority, and behavior management in administration as she analyzed the limiting variables affecting the cyber security assessment framework in Kenyan government ministries. The current study, which also takes into account the leadership and human elements involved in the implementation of cyber security frameworks, is related to this research.

In order to address system vulnerabilities and subsequent cyber-attacks, human and organizational components of information systems security have been neglected in favor of technological ones. (Dhillon and Backhouse, 2021). Due to the constant interaction of organizational and human elements with systems and technology, key systems must be protected. (Rasmussen, 2014; Reason, 2017). The efficiency of ICT security in a company is influenced by management engagement, the existence of a security policy (Kankanhalli et al., 2013), staff training and awareness (Bulgurcu, Cavusoglu & Benbasat, 2020), and staff training and awareness. Governmental entities are also becoming more reliant on IS. An effective, private, and reliable information system is essential for a government to maintain social and economic stability as well as to be globally competitive. Unsecure information systems in the public sector can have a detrimental impact on the people's trust and willingness to use governmental entities, which can undermine economic and social stability. (Tarimo, 2016).

Identifying the ICT assets and exposure involved, implementing and adhering to cyber security strategy and standards, improving responsiveness to frequent technological changes and threats there-off, human factor in addressing awareness and the arising vulnerabilities, and leadership as critical in the study for positive change in cyber security strategy, human factor, and leadership are identified as key factors to a successful cyber security by Pelgrin (2014).

This study will be conducted in a global environment with a focus on wealthy countries, therefore its relevance to developing countries and the public sector may be restricted. Insiders can be broadly categorized into three groups who occasionally launch cyberattacks: (i) employees who are seeking retribution for "unfair" treatment within the organization; (ii) insiders who are using the company's resources for their own personal gain; and (iii) unintended cyber-attacks insiders who are primarily not the attackers but who unwittingly facilitate outside attacks. (Andress & Winterfeld, 2021).

Summary of Empirical Review

The present body of research on cyber security in the public sector underlines how important it is for decision-makers to comprehend the implications of e-governments and how they interact with current systems. Organizations must inventory their key infrastructure assets in order to create a strong cyber security strategy, as an organization cannot defend its assets if it is not aware of them. The sources and characteristics of cyber risks can also be determined by understanding the information systems assets of a company, allowing for sufficient planning.

Since a system is only as strong as its weakest link, managers must assess organizational and human variables that may result in cyber security weaknesses. Previous research has uncovered elements including employee awareness, management commitment to strategy and policies, organizational structure (particularly information systems structure), implementers' abilities and training in cyber security, and employees' ethical behavior.

There has not been much research done on the difficulties with information security in e-government, particularly in the context of emerging and East African nations. Prior e-government research has mostly concentrated on the design, adoption, and development phases. This study aims to fill the knowledge gap about the elements that influence cyber security in Kenyan public sector organizations.

Review Observations

The public sector, including the government and related parastatals, is at the greatest danger level for cyberattacks, (Serianu 2015). Loss of intellectual property, financial loss, the disclosure of sensitive customer information, disruption of business operations, increased costs for system recovery, loss of stakeholder confidence, loss of competitive advantage, disclosure of operational strategies, and possibly job loss or organizational extinction are all possible outcomes of a breach in cyber security. Cyberattack losses in Kenya totaled more than KES 5 billion for the governmental sector, KES 4 billion for the financial services industry. Developing nations are making significant investments in e-government, yet insecure e-government systems can have a severe impact on stakeholder confidence and service delivery. E-government security is essential for fostering reliability and confidence in service delivery. Due to their various operational contexts and requirements, effective cyber security aspects in e-government services may be different from those in the private sector. Cyber security considerations can be divided into two categories: internal system flaws or vulnerabilities that attackers can take advantage of, and external motivating reasons for attackers.

The extensive accessibility of the internet has improved its usability for authorized users, but it has also exposed crucial infrastructure to cyberattacks from unauthorized users. Against its adversaries, especially other states, state agencies have been exploiting the internet as a weapon. Based on the motivations of the attackers, cyberattacks can be divided into four primary categories: hacking exploitation, serious and organized crime, ideological and political extremism, and state-sponsored cyber aggression. Different interests, such as those related to economics, politics, and national security, are behind these attacks (Cornish, 2019). Even though the attacker pretends to have a cause, the true motivations behind these attacks are frequently concealed or obfuscated. Today, extremist organizations use the internet to recruit new members, plan physical assaults, find funding, and disseminate propaganda. The primary driver behind non-political system attacks is financial gain. For efficient cyber security planning and implementation. According to Cornish (2019) underlines the significance of categorizing and prioritizing different sources of cyber-attacks. In order to ensure successful cyber security planning and implementation, it is imperative to examine the primary driving forces behind cyber attackers in relation to an organization's systems.

CONCLUSION OF REVIEW

The findings of this study would be very valuable to policymakers as they would offer direction when creating strategies and regulations that have an impact on certain internet users. The study's results can also be used by information security experts to decide how to address cyber threats.

The study's analysis of the model's flaws and suggestions for enhancements against nefarious insiders and outsiders may be useful to those working in critical infrastructure and security organizations tasked with protecting critical assets. The study's results would add to what is already known about cybercrime in Kenya's public sector. The study may also help future researchers and scholars pinpoint potential areas of study on cyber security in the public sector. The results of the study would also be a crucial tool for future research.

REFERENCES

Alfawaz, S, May, LJ & Mohanak, K 2008, 'E-government security in developing countries: a managerial conceptual framework', paper presented to International Research Society for Public Management Conference, Queensland University of Technology, Brisbane, 26-28 March 2008.

Bougaardt, G and Kyobe, M. “Investigating the Factors Inhibiting SMEs from Recognizing and Measuring Losses from Cyber Crime in South Africa” *The Electronic Journal Information Systems Evaluation* Volume 14 Issue 2 2011, (pp167-178),

Brenner, S., W. (2002b). The privacy privilege: Law enforcement, technology and the constitution. *Journal of Technology Law and Policy* 7 (2) 123-94.

Brenner, S.,W. (2004). Toward a criminal law for cyberspace, Distributed Security. Boston University *Journal of Science & Technology Law* 10 (2).

Bulgurcu, B., Cavusoglu, H., &Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,*MIS Quarterly*34(3), 523-548.

Chang and C-S. Lin (2007) "Exploring organizational culture forinformation security management," *Industrial Management & DataSystems*, vol. 107, no. 3, pp. 438-458.

Chau, P. Y., Kuan, K. K., & Liang, T. (2007). Research on IT value: What we Have Done in Asia and Europe. *European Journal of Information Systems*,*16*(3), 196.

Cooper, D.R., & Schindler, P.S. (2003). Business Research Methods. (8th ed.). Boston: 15 McGraw-Hill Irwin.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches*. Sage.

Dacin, M. T., Goodstein, J., & Scott, W. R. (2002). Institutional Theory and institutional Change: Introduction to the Special Research Forum. *Academy of Management Journal*, *45*(1), 45-56.

Dhillon, G., &Torkzadeh, G. (2006). Value-focused Assessment of Information Systems Security in Organizations, *Information Systems Journal*16(3), 293314.

Einhorn, H. J., & Hogarth, R. M. (1981). Behavioral Decision Theory: Processes of Judgment and Choice. *Journal of Accounting Research*, 1-31.

Glenny, M., Glick, B., & Wainwright, R. (2010). Cybercrime, cybersecurity and the future of the internet.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations.*European Journal of Information Systems*18(2), 106-125.

Hulme, G. V. (2011). SCADA Insecurity-Stuxnet put the Spotlight on Critical Infrastructure Protection but Will Efforts to Improve it come too late?*Information Security Magazine*, 13(1), 38-44.

International Telecommunication Union (2004). Understanding Cybercrime: A Guide for Developing Country.

Jin, X. Q. Z. G. C. (2006). Theoretical Trace and Framework of Overall Innovation Management. *Chinese Journal of Management*, *2*, 002.

Kankanhallia, A., Teo, H., Tan, B., & Wei, K. (2003). An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management* (23), 139-154.

Kimutai, J. K. (2014). *Social media and national security threats: a case study of Kenya*. (Doctoral dissertation, University of Nairobi).

King'ori, P. M. (2014). *Assessment of Awareness and Preparedness of Cyber cafe Internet Users to deal with threats of cyber-crimes: A case of Nairobi County* (Doctoral dissertation, University of Nairobi).

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International.

Kyobe, M. (2008). Evaluating Information Security within SMEs engaged in Ecommerce in South Africa. *Institute for Small Business & Entrepreneurship*, 5-7.

Magutu, P.A., Ondimu, G.M., &Ipu, C.J. (2011) Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya, *Journal of Information Assurance & Cyber security*.

Mugenda, A. G. (2008). Social Science Research: Theory and Principles *Nairobi: Applied*.

Nerey H.M.M. (2012). Information System Security Effectiveness Attributes: A Tanzanian Company Case Study. *World Academy of Science, Engineering and Technology* (70), 551-557.

Nyawanga, J. O. (2015). *Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector* (Doctoral dissertation, University of Nairobi).

Olayemi, O. J. (2014). A socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria, *International Journal of Sociology and Anthropology*, 6(3), 116-125.

Osang, F. B., Ngole, J. &. Tsuma C (2013). Prospects and Challenges of M-learning Implementation In Nigeria: Case Study National Open University Of Nigeria (NOUN). International Conference on ICT for Africa.

Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th Design Automation Conference* (pp. 731-736). ACM.

Ruighaver, A. B., Maynard, S., B. & Chang, S. (2007). Organizational Security Culture: Extending the End-User Perspective. *Computers & Security*, 26 (1), 56-62.

Santos, T. P. (2010). A Security Audit Framework to Manage Information System Security. *ICGS*(3),

Serianu Consultants in Cyber Security (2015); available at ahttp://www.usiu.ac.ke/oncampus/news/296-serianu-usiu-africa-pkf-consulting-launch-kenya-cybersecurity-report-2015

Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its Challenges to Society, *International Journal of Scientific & Engineering Research*, 3(6), 124-132

Siponen, Pahnila, and Mahmood (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer* 43(2), 64-71.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavioral Decision Theory. *Annual Review of Psychology*, *28*(1), 1-39.

Solms R. and Solms B. (2004). "From policies to culture," *Computers & Security*, vol. 23, no. 4, pp. 275-279, 2004.

Straub, D. (1990). "Effective IS Security," *Information Systems Research*, vol. 1, no. 3, pp. 255-273.

Straub, D. (1990). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly* 22(8), 441-465.

Tarimo, C. (2006): ICT Security Readiness Checklist for Developing countries: A Social-Technical Approach. Ph.D thesis. Stockholm University, Royal Institute of Technology.

Tonge, A. M., Kasture, S. S., and Chaudhari, S. R. (2013). Cyber Security: Challenges for Society- Literature Review, *Journal of Computer Engineering*, 12(2), 67-75

Wechuli A. (2014) on Cyber Security Assessment Framework: Case of government Ministries in Kenya; *International Journal of Technology in Computer Science and Engineering*, 1(3).

Wekundah, R. N. (2015). *The effects of cyber-crime on e-commerce; a model for SMEs in Kenya* (Doctoral dissertation, University of Nairobi).

Zanoon, N., Albdour, N., & Hamatta, H. S. (2015) Security challenges as a factor affecting the security of manet: attacks, and security solutions. International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015

Zhu, K., Kraemer, K. L., &Xu, S. (2002). A Cross-Country Study of Electronic Business Adoption Using the Technology-Organization-Environment Framework.