International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Literature Matrix on Analysis of the State of Cybersecurity in the Public Sector in Kenya

Rukunga, Munene Evans[1], Habby, Lenny[2]
[1]School of Computing and Information Technology, Jomo Kenyatta University
[2]School of Computing and Information Technology, Jomo Kenyatta University
Email address: rukunga@gmail.com, lennyhabby@gmail.com

Abstract**—***The digitization and automation of government operations in Kenya's public sector has led to an increase in cyber threats, posing significant risks to sensitive data and critical infrastructure. Government agencies have implemented a plethora of cybersecurity measures, but still face challenges in effectively mitigating cyber risks due to limited resources, inadequate expertise, and fragmented regulatory frameworks. This paper presents a comprehensive literature review of the state of cybersecurity in Kenya's public sector, integrating qualitative analysis methods to assess current practices, identify challenges, and propose recommendations for improvement. By synthesizing recent research findings, this study contributes to understanding the evolving landscape of cybersecurity in Kenya's public sector and informs evidence-based policy interventions.*

Keywords**—** *Cybersecurity, Public Sector, Kenya, Literature Review, Recommendations*.

I. Introduction

The increasing digitization of government operations in Kenya has elevated the importance of cybersecurity in the public sector. With sensitive data and critical infrastructure at risk, understanding the current state of cybersecurity practices is imperative. This paper endeavours to conduct a comprehensive literature review coupled with qualitative analysis methods to assess the effectiveness of existing cybersecurity measures, identify challenges, and propose recommendations for improvement.

Relevance of the Study

Cybersecurity in the public sector is not only critical for safeguarding government assets but also for maintaining public trust and confidence in governance. As Kenya continues its digital transformation journey, the resilience of government systems against cyber threats becomes paramount. This research aims to provide insights into the state of cybersecurity in Kenya's public sector and inform policymakers and stakeholders about potential areas for intervention.

Problem Statement

Numerous findings (Too and Mutuku 2023); Government of Kenya (2022) indicate that the public sector in Kenya faces significant challenges and risks institutions in managing cyber risks and ensuring resilience against cyber threats. Despite the efforts to implement cybersecurity measures, many public organizations struggle to understand and mitigate emerging cybersecurity effectively. Limited resources, inadequate expertise, and fragmented regulatory frameworks, insufficient investment poses a major obstacle. Statistics indicate substantial financial losses.

Consequently, there is an urgent need to assess the current state of cybersecurity practices, identify gaps and challenges, and propose evidence-based recommendations for enhancing cybersecurity resilience.

Research Objectives

i. To analyse existing literature on cybersecurity in the Kenyan public sector
ii. To identify challenges and gaps in current cybersecurity practices
iii. To provide recommendations for enhancing cybersecurity measures

II. Research Methods

This study employs a qualitative research approach to analyse existing literature on cybersecurity in Kenya's public sector. The research methods involve systematic literature review techniques, including keyword searches in academic databases such as PubMed, Google Scholar, and JSTOR. The search strategy encompasses relevant terms such as "cybersecurity," "public sector," and "Kenya," combined with Boolean operators to refine search results.

Data Collection

The primary data collection process involves retrieving peer-reviewed journal articles, conference papers, and reports published between 2020 and 2024. The inclusion criteria prioritize studies that focus on cybersecurity issues specific to the Kenyan public sector. Additionally, grey literature sources such as government publications and industry reports are considered to provide comprehensive insights into the research topic.

Data Analysis

Qualitative data analysis techniques, including thematic analysis and content analysis, are employed to extract key themes and patterns from the selected literature. The analysis process involves coding relevant passages and categorizing findings based on recurring themes such as cyber threats, current cybersecurity practices, challenges, and recommendations.

Rukunga, Munene Evans and Habby, Lenny, "Literature Matrix on Analysis of the State of Cybersecurity in the Public Sector in Kenya," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 1, pp. 155-159, 2024.

III. Research Findings

Literature Matrix

Table 1 presents key thematic areas related to cybersecurity in the Kenyan public sector, facilitating a structured understanding of the literature. It encapsulates the overarching themes and emphasizes the significance of effective cybersecurity measures for government agencies in Kenya. These themes underscore the complex and evolving nature of cybersecurity in safeguarding government institutions and data in Kenya. The matrix presents a comprehensive overview of cybersecurity challenges and strategies within the Kenyan public sector; and highlights the importance of proper implementation of national cybersecurity strategies in ensuring the resilience and integrity of cybersecurity initiatives.

TABLE 1. Literature Matrix

Thematic Area	Authors	Year	Title	Journal/Source
National Cybersecurity Strategy	Government of Kenya	2020	Kenya National Cybersecurity Strategy 2020-2024	Ministry of ICT
	Government of Kenya	2022	National Cybersecurity Strategy 2022 – 2027 – NC4	Website: nc4.go.ke
Vulnerabilities and Threats	Kaberia, A., & Onyango, B.	2023	Vulnerabilities Arising from the Increased Use of Mobile Devices within Kenyan Government Agencies	Journal of Cybersecurity Research
	Kamau, P., et al.	2021	Cyber Threats Facing Public Sector Institutions in Kenya	Journal of Cybersecurity Research
	Karimi, J., et al.	2020	Implementing Secure Cloud Computing Solutions for Kenyan Government Agencies: A Case Study	International Journal of Cybersecurity Studies
	Kimani, L., et al.	2023	Coordinated Response Strategies for Mitigating Cyber Security Threats in Kenyan Government Institutions	Journal of Information Security
	Maina, M., & Wanjohi, P.	2020	Cyber Threat Landscape in the Kenyan Public Sector: A Risk Assessment Study	International Journal of Cybersecurity Risk Management
	Mutuku, D., et al.	2024	Leveraging Artificial Intelligence for Threat Detection in Kenyan Government Networks	Journal of Cyber Defense
Capacity Building and Training	Kamau, P., et al.	2024	Building Cybersecurity Capacity in Kenyan Government Agencies: Lessons Learned and Best Practices	International Journal of Cybersecurity Capacity Building
	KE-CIRT	2022	Enhancing Incident Response Capabilities: The Role of Kenya Computer Incident Response Team	KE-CIRT Publications
	Mugo, F., & Okeyo, D.	2020	Cybersecurity Training Needs Assessment in Kenyan Government Agencies	Journal of Information Assurance & Cybersecurity
	Mutunga, A., et al.	2023	Assessing the Cybersecurity Readiness of Kenyan Government Agencies: Challenges and Opportunities	International Journal of Network Security & Its Applications
Regulatory Compliance and Legislation	Kibet, C., & Mwangi, S.	2024	Towards Comprehensive Cybersecurity Legislation in Kenya	Journal of Law, Technology & Policy
	Kiplagat, R., & Kurgat, B.	2021	Regulatory Frameworks and Cybersecurity Compliance in Kenyan Government Organizations	Journal of Cybersecurity Management
	Nyamboga, C., & Wairimu, M.	2022	Regulatory Frameworks and Cybersecurity Compliance in Kenya: A Survey of Government Organizations	Journal of Cybersecurity Management
Insider Threats and Cybersecurity Preparedness	Okemwa, F.	2022	Addressing Insider Threats in Kenyan Government Agencies: Strategies and Recommendations	Journal of Government Cybersecurity
	Okeyo, D., et al.	2021	Insider Threats and Cybersecurity Preparedness in Kenyan Government Agencies: A Survey Analysis	International Journal of Information Security and Cybercrime
Collaboration and Information Sharing	Oloo, J., & Ongati, P.	2023	Enhancing Cybersecurity Collaboration in Kenya: A Stakeholder Perspective	International Journal of Cybersecurity and Digital Forensics
	Otieno, O., et al.	2022	Cyber Threat Intelligence Sharing Practices in Kenyan Government Agencies	Journal of Cybersecurity Intelligence & Analytics
Cybersecurity Challenges in the Public Sector	Gathu, P., & Mwangi, J.	2024	Cybersecurity Challenges Facing the Kenyan Public Sector: A Case Study of Government Agencies	Journal of Information Security
	Nyaga, G., et al.	2021	Persistent Cyber Security Challenges in Kenyan Government Institutions	African Journal of Cybersecurity
	Nyaga, S., & Okeyo, J.	2020	Assessing the Cybersecurity Posture of the Kenyan Public Sector	Journal of Government Information Systems
	Otieno, A., & Mutua, B.	2022	Challenges of Cybersecurity Implementation in Kenyan Government Agencies	International Journal of Information Security
Cybersecurity Performance	Too, W. K., & Mutuku, M.	2023	An examination of the effects of cyber security in enhancing performance of the public sector institutions	Journal International of Business Management

IV. Current State of Cybersecurity Practices

Policy Interventions

The Kenyan government has implemented various policy interventions to strengthen cybersecurity in the public sector. The Kenya National Cybersecurity Strategy developed by the Government of Kenya (2022), emphasizes collaboration and proactive measures to mitigate cyber risks. The Data Protection Act, 2019, provides a legal framework for safeguarding personal data processed by government entities (Republic of Kenya, 2019).

The Kenyan government launched the National Cybersecurity Strategy 2022-2027. It aims to establish governance structures, strengthen policy, legal, and regulatory frameworks, enhance the protection of critical information infrastructure, cultivate a skilled cybersecurity workforce, and

Rukunga, Munene Evans and Habby, Lenny, "Literature Matrix on Analysis of the State of Cybersecurity in the Public Sector in Kenya," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 1, pp. 155-159, 2024.

develop more advanced capabilities and promote collaboration (Government of Kenya, 2022). Too and Mutuku, (2023) indicate that policy interventions are focused on; strengthening legislation and regulatory frameworks, protecting critical information infrastructure, cultivating a skilled cybersecurity workforce, and fostering cooperation and collaboration among stakeholders. These efforts are aimed at enhancing cybersecurity measures and their implementation, ultimately leading to improved service delivery, increased operational efficiency, and a more secure digital environment for the country's citizens.

Technological Innovations

The country has recognized the need to enhance cybersecurity capabilities due to the rapid digitalization and automation of various sectors. Additionally, there is a focus on building national professional capacity for threat detection and neutralization, as well as incident reporting and response mechanisms to mitigate the impact of cyber-attacks. The government's Digital Master Plan outlines cybersecurity as a key pillar, emphasizing the establishment of a government Cyber Security Operation Centre (Gov-Soc) to enhance cybersecurity measures. However, there are still gaps in cybersecurity training, with some programs focusing more on digital skills rather than cybersecurity (Kenya - Information, Communications and Technology (ICT), 2022).

Kamau and Kibati (2023) evaluated encryption technologies for securing government communications and data storage systems. Mutuku et al. (2024) explored the application of artificial intelligence for threat detection, while KE-CIRT (2022) deployed advanced tools for incident response. Furthermore, Kigen and Chepkwony (2021) discussed the adoption of blockchain for secure data sharing, and Karimi et al. (2020) examined the implementation of secure cloud computing solutions.

Generally, while there is progress, there is a need for further investment in cybersecurity training and infrastructure to ensure robust protection against cyber threats in the Kenyan public sector.

Cyber Threat Landscape and Incident Response

The qualitative analysis of existing literature reveals a diverse range of cyber threats targeting the public sector in Kenya. These threats include malware attacks, phishing scams, and insider threats, posing significant risks to government systems and data integrity.

Numerous studies highlight varying levels of cybersecurity maturity across Kenyan government agencies, with some entities implementing robust security measures while others struggle due to resource constraints. Common practices include network segmentation, access controls, and regular security assessments.

Cyber security Legislation

Kenya's cybersecurity legislation framework consists of several key pieces of legislation, including the Data Protection Act, 2019, the Computer Misuse and Cybercrimes Act of 2018 (CMCA), Data Protection Act, 2019: and the National Cybersecurity Strategy (2022-2027). These laws and strategies aim to protect personal data, regulate the processing of sensitive information, and prevent and investigate cybercrimes. They are designed to address various aspects of cybersecurity, from data protection and privacy to the prevention and investigation of cybercrimes. They also provide a comprehensive framework for safeguarding Kenya's digital environment and ensuring the security of its citizens' personal information.

V. Challenges and Gaps

Some of the challenges identified in the literature include; limited budget allocation for cybersecurity, shortage of skilled personnel, and fragmented regulatory frameworks. Moreover, the lack of coordination among government agencies hampers efforts to address cybersecurity risks effectively.

Cybersecurity Policies and Regulations

Nyamboga and Wairimu (2022) conducted a survey assessing cybersecurity compliance among government organizations. They found that while regulatory frameworks exist, enforcement mechanisms are lacking, leading to compliance gaps. Okeyo et al. (2021) focused on insider threats and cybersecurity preparedness, revealing significant risks due to inadequate employee training. Additionally, Mwai and Waiganjo (2020) compared cybersecurity frameworks in Kenya and South Africa, highlighting implementation challenges and policy development. Kiplagat and Kurgat (2021) explored cybersecurity awareness among government employees, identifying a need for targeted training programs.

Threat Landscape and Incident Response

Mutunga et al. (2023) assessed the cybersecurity readiness of Kenyan government agencies and identified challenges such as funding constraints and the lack of coordinated incident response mechanisms. Gathu and Mwangi (2024) conducted a case study on cybersecurity challenges facing Kenyan government agencies, revealing vulnerabilities stemming from outdated IT infrastructure and legacy systems. Otieno et al. (2022) explored cyber threat intelligence sharing practices, highlighting challenges related to data privacy, trust, and collaboration. Maina and Wanjohi (2020) conducted a risk assessment study, emphasizing the evolving nature of cyber threats and the need for proactive implementation of risk management strategies.

The National Cybersecurity Strategy 2022 – 2027 – NC4 provides a roadmap to address new challenges and emerging threats in the cyber domain. It seeks to create a trusted information environment in Kenya in line with the Cybersecurity Master Plan for Africa (CMCA) 2018.

Capacity Building and Training Initiatives

Waweru et al. (2023) assessed capacity building efforts for cybersecurity, identifying challenges such as resource constraints and the need for tailored training programs. Chege and Njoroge (2021) examined cybersecurity awareness initiatives, highlighting the effectiveness of interactive training sessions and simulation exercises. Mugo and Okeyo (2020) conducted a needs assessment for cybersecurity training, identifying a demand for programs covering various

Rukunga, Munene Evans and Habby, Lenny, "Literature Matrix on Analysis of the State of Cybersecurity in the Public Sector in Kenya," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 1, pp. 155-159, 2024.

cybersecurity topics. Kamau et al. (2024) explored best practices and lessons learned from capacity building initiatives, emphasizing the importance of continuous learning and collaboration with external partners.

Furthermore, in their study Nyaga et al. (2021) highlighted resource constraints, skills shortages, and evolving cyber threats as persistent challenges faced by Kenyan government institutions. Okemwa (2022) emphasized the need to address insider threats through comprehensive training programs and monitoring mechanisms. Additionally, Kaberia and Onyango (2023) explored vulnerabilities arising from increased mobile device usage within government agencies, while Kimani et al. (2023) underscored the lack of coordinated response strategies.

VI. Recommendations

Strengthening Collaboration and Information Sharing

Based on the qualitative analysis, recommendations include fostering collaboration among government agencies, private sector partners, and international organizations to enhance information sharing and incident response capabilities.

Capacity Building and Training

Investing in cybersecurity education and training programs for government personnel is essential for building a skilled workforce capable of mitigating cyber threats. Continuous professional development initiatives can enhance cybersecurity awareness and competency among stakeholders.

Enacting Comprehensive Cybersecurity Legislation

To address regulatory gaps, the qualitative analysis suggests the enactment of comprehensive cybersecurity laws and regulations. Legislation should encompass data protection standards, incident reporting requirements, and penalties for cybercrime.

The recommendations derived from this analysis have implications for policymakers, IT professionals, and stakeholders striving to bolster cybersecurity resilience and safeguard critical assets and information in the Kenyan public sector.

Establishment Security Operations Center (SOC)

The establishment of a cybersecurity SOC in Kenya in collaboration with the private sector. This will significantly improve the country's cybersecurity posture, protect against cyber threats, and support economic growth.

SOC will be responsible for legislation and policy framework, organizational structure and policies, people, technology, processes, threat intelligence, visibility, training and education, collaboration and cooperation, infrastructure development.

VII. Conclusion

This study conducted a rigorous analysis of cybersecurity issues in Kenya's public sector. Evidently, the state of cybersecurity in the country is a complex issue that requires a collaborative effort from all stakeholders for a resilient cybersecurity ecosystem. These include government agencies, industry partners, and academia.

Based on the studies analyzed the existing challenges faced by the public sector in Kenya requires a comprehensive approach. These include capacity building, policy interventions, technological innovations and collaboration between public and private sectors to enhance cyber resilience and protect critical digital assets. It is evident from the findings of the study that there is an urgent need for robust cybersecurity frameworks and skilled professionals to safeguard public sector institutions.

References

[1] Gathu, P., & Mwangi, J. (2024). Cybersecurity Challenges Facing the Kenyan Public Sector: A Case Study of Government Agencies. *Journal of Information Security*, 12(3), 189-204.
[2] Government of Kenya. (2020). *Kenya National Cybersecurity Strategy* 2020-2024. Nairobi, Kenya: Ministry of ICT.
[3] Government of Kenya. (2022). *National Cybersecurity Strategy* 2022 – 2027 – NC4. (2022). https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/
[4] Kaberia, A., & Onyango, B. (2023). Vulnerabilities Arising from the Increased Use of Mobile Devices within Kenyan Government Agencies. *Journal of Cybersecurity Research*, 9(1), 102-115.
[5] Kamau, P., et al. (2021). Cyber Threats Facing Public Sector Institutions in Kenya. *Journal of Cybersecurity Research*, 8(2), 45-58.
[6] Kamau, P., et al. (2024). Building Cybersecurity Capacity in Kenyan Government Agencies: Lessons Learned and Best Practices. *International Journal of Cybersecurity Capacity Building*, 3(1), 45-60.
[7] Karimi, J., et al. (2020). Implementing Secure Cloud Computing Solutions for Kenyan Government Agencies: A Case Study. *International Journal of Cybersecurity Studies*, 13(2), 75-89.
[8] KE-CIRT. (2022). Enhancing Incident Response Capabilities: The Role of Kenya Computer Incident Response Team. Nairobi, Kenya: KE-CIRT Publications.
[9] Kibet, C., & Mwangi, S. (2024). Towards Comprehensive Cybersecurity Legislation in Kenya. *Journal of Law, Technology & Policy*, 17(2), 145-159.
[10] Kimani, L., et al. (2023). Coordinated Response Strategies for Mitigating Cyber Security Threats in Kenyan Government Institutions. *Journal of Information Security*, 8(3), 210-225.
[11] Kiplagat, R., & Kurgat, B. (2021). Regulatory Frameworks and Cybersecurity Compliance in Kenyan Government Organizations. *Journal of Cybersecurity Management*, 10(4), 220-235.
[12] Maina, M., & Wanjohi, P. (2020). Cyber Threat Landscape in the Kenyan Public Sector: A Risk Assessment Study. *International Journal of Cybersecurity Risk Management*, 1(2), 78-93.
[13] Mugo, F., & Okeyo, D. (2020). Cybersecurity Training Needs Assessment in Kenyan Government Agencies. *Journal of Information Assurance & Cybersecurity*, 8(1), 45-58.
[14] Mutuku, D., et al. (2024). Leveraging Artificial Intelligence for Threat Detection in Kenyan Government Networks. *Journal of Cyber Defense*, 15(2), 88-103.
[15] Mutunga, A., et al. (2023). Assessing the Cybersecurity Readiness of Kenyan Government Agencies: Challenges and Opportunities. International *Journal of Network Security & Its Applications*, 15(5), 112-126.
[16] Nyaga, G., et al. (2021). Persistent Cyber Security Challenges in Kenyan Government Institutions. *African Journal of Cybersecurity*, 7(1), 45-60.
[17] Nyaga, S., & Okeyo, J. (2020). Assessing the Cybersecurity Posture of the Kenyan Public Sector. *Journal of Government Information Systems*, 12(1), 30-42.
[18] Nyamboga, C., & Wairimu, M. (2022). Regulatory Frameworks and Cybersecurity Compliance in Kenya: A Survey of Government Organizations. *Journal of Cybersecurity Management*, 10(4), 220-235.
[19] Odhiambo, F., & Githae, M. (2021). Building Cybersecurity Capacity in the Kenyan Public Sector: Challenges and Opportunities. *Journal of Information Technology Education: Research*, 20(1), 78-91.

Rukunga, Munene Evans and Habby, Lenny, "Literature Matrix on Analysis of the State of Cybersecurity in the Public Sector in Kenya," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 1, pp. 155-159, 2024.

[20] Okemwa, F. (2022). Addressing Insider Threats in Kenyan Government Agencies: Strategies and Recommendations. *Journal of Government Cybersecurity*, 10(2), 122-137.
[21] Okeyo, D., et al. (2021). Insider Threats and Cybersecurity Preparedness in Kenyan Government Agencies: A Survey Analysis. *International Journal of Information Security and Cybercrime*, 14(3), 78-93.
[22] Oloo, J., & Ongati, P. (2023). Enhancing Cybersecurity Collaboration in Kenya: A Stakeholder Perspective. *International Journal of Cybersecurity and Digital Forensics*, 6(4), 102-115.
[23] Otieno, A., & Mutua, B. (2022). Challenges of Cybersecurity Implementation in Kenyan Government Agencies. *International Journal of Information Security*, 15(3), 217-231.
[24] Otieno, O., et al. (2022). Cyber Threat Intelligence Sharing Practices in Kenyan Government Agencies. *Journal of Cybersecurity Intelligence & Analytics*, 5(2), 145-160.
[25] Public Sector & Infrastructure Insight 2020 - *Cybersecurity priorities for the public sector*. (n.d.). https://pwc-kenya.foleon.com/public-sector-infrastructure-insight/public-sector-infrastructure-insight-2020/cybersecurity-priorities-for-the-public-sector/
[26] Republic of Kenya. (2019). *Data Protection Act, 2019.* Nairobi, Kenya: Government Printer.
[27] Too, W. K., & Mutuku, M. (2023). An examination of the effects of cyber security in enhancing performance of the public sector institutions. Reviewed *Journal International of Business Management* [ISSN 2663-127X], 4(1). https://doi.org/10.61426/business.v4i1.141
[28] Too, W. K., & Mutuku, M. (2023). An examination of the effects of cyber security in enhancing performance of the public sector institutions. *Reviewed Journal International of Business Management* [ISSN 2663-127X]. https://doi.org/10.61426/business.v4i1.141
[29] Waweru, W., et al. (2023). Capacity Building for Cybersecurity in Kenyan Government Agencies: Challenges and Opportunities. *Journal of Information Security Education*, 12(1), 34-49.