IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 3, Ser. 2 (May. – June. 2025), PP 13-18
www.iosrjournals.org

Effects Of Cybersecurity Vulnerabilities On ICT Systems In County Governments In Kenya

Kadima Victor Chitechi [1] Preston Simiyu[2] Stephen Gitonga [3]
[1, 2,3] *Department Of Information Technology, Masinde Muliro University Of Science And Technology*

Abstract
The proliferation of modern computer technologies and internet connectivity has enhanced societal functions and service delivery, but has also led to a surge in cyber-attacks. Many computer systems are susceptible to exploitation due to inadequate security protocols, including weak passwords, outdated software, and insufficient firewalls. This has resulted in a high prevalence of malware attacks, particularly affecting critical infrastructure in Kenya, such as government financial systems. The exploitation of these vulnerabilities by cyber-attackers has caused substantial losses, underscoring the necessity for enhanced cybersecurity measures, especially within Kenyan county governments.

Keywords: *Cybersecurity, vulnerability, ICT, Systems, Effects.*

Date of Submission: 01-05-2025 Date of Acceptance: 10-05-2025

I. Introduction

The integration of modern computer technologies and internet connectivity has significantly enhanced societal functions; however, this advancement has been accompanied by a surge in cyber-attacks, posing serious threats to computer systems. A lack of proper security measures, including the absence of strong passwords, reliance on unlicensed and outdated antivirus software, and insufficient firewalls, coupled with the failure to update operating systems, leaves systems vulnerable to exploitation [3]. These vulnerabilities, defined as weaknesses in the design, implementation, or operation of computer systems, are a key concern, as highlighted by reports indicating a substantial percentage of organizations experiencing malware attacks. A computer system breach may cause serious losses and risks to confidential data and may lead to system failure [1]

Cybersecurity safeguards computer systems by preventing unauthorized access, misuse, damage, or loss of electronic information, software, and hardware. The challenges in cybersecurity are constantly changing because malicious actors are always discovering new system weaknesses. These actors are both improving their skills and using increasingly sophisticated technology and methods to attack various organizations [2].

These vulnerabilities are a key threat because they can be exploited by network attacks, posing serious risks. Some users within organizations may also pose insider threats, either directly or indirectly facilitating network attacks [2]. The challenge is compounded by the fact that many organizations struggle to implement effective cybersecurity measures to counter these evolving cyber-attacks. Cybersecurity, which encompasses measures designed to protect computer systems against unauthorized access or attack, is critical, but its effectiveness is often undermined by the emergence of new and sophisticated threats.

The term "cyber" refers to the digital world of interconnected networks and information systems, often called "virtual reality." Cybersecurity is the practice of protecting the confidentiality, integrity, and availability of data and assets both physical and digital within this electronic environment, as established by institutions, organizations, and individuals [1]

Cybersecurity is a broad discipline focused on protecting digital systems, networks, devices, and data from malicious attacks. While related concepts like data security, information security, and network security share similar goals, each has a more specific focus [4]. Data security is concerned with preventing unauthorized access, alteration, or disclosure of digital data throughout its lifecycle. Information security focuses on safeguarding both physical and digital information by ensuring its confidentiality, integrity, and availability. Network security, on the other hand, aims to protect data as it travels across communication networks. Unlike these more targeted areas, cybersecurity provides a comprehensive approach, covering end-to-end protection across all components of the digital environment [4].

Vulnerabilities are weaknesses or flaws found in software, hardware, or systems that can be exploited by attackers to undermine security [1]. These flaws may be present in elements like code, system configurations, or overall design, leaving systems open to threats such as unauthorized access or data breaches. Managing these vulnerabilities is a vital part of cybersecurity and involves measures such as routine software updates, effective patch management, and adherence to security best practices to minimize the risk of exploitation [1].

In Kenya, this issue is particularly acute, with government systems, including those managing critical financial transactions, increasingly targeted by cyber-attacks. For instance, several government departments have suffered attacks, with hackers exploiting vulnerabilities in key systems. These attacks, often attributed to 'cyber-terrorists' taking advantage of weaknesses in systems like the Integrated Financial Management Information System (IFMIS), have resulted in significant financial losses and disruption of essential services. The situation is worsened by the fact that many organizations, including banks, have been slow to adopt robust security measures like data encryption, leaving them highly exposed to cyber-criminals [5].

The rise in cyber-attacks is a major concern for governments worldwide, including Kenya, where both government and private sectors have seen a dramatic increase in such incidents. Reports indicate that critical cybersecurity infrastructure and new technological advancements are particularly vulnerable. Moreover, sectors such as electronic banking and online portals that handle credit transactions are often inadequately protected, making them easy targets for attackers. The lack of proactive cybersecurity initiatives at the county government level further exacerbates the problem, highlighting the urgent need for comprehensive strategies to mitigate the growing threat of cyber insecurity in Kenya [5].

The Global Cybersecurity Index (GCI), developed by the International Telecommunication Union (ITU), is a ranking system designed to assess countries' commitment to cybersecurity on a global scale. Its main objective is to help nations enhance their cybersecurity preparedness and resilience by providing a benchmark for comparison and promoting international collaboration. The GCI aims to evaluate efforts to strengthen cybersecurity, encourage the adoption of best practices, identify weaknesses in national strategies, support capacity-building initiatives, and ultimately contribute to improving global cybersecurity resilience [5].

II. Cybersecurity In Kenya

As Kenya undergoes a rapid digital transformation, cybersecurity has become a major concern for both the public and private sectors. With the rise in internet access and widespread adoption of digital technologies across various industries, the country faces escalating cyber threats that pose significant risks to its economic growth and development objectives. This situation underscores the pressing need to address vulnerabilities in the country’s cybersecurity infrastructure, particularly in the ICT systems of county governments. Failure to do so could result in significant disruptions to public services, financial losses, and loss of public trust in government institutions [6].

Kenya has experienced remarkable progress in digital adoption over the past decade. By September 2023, internet penetration reached 94.4%, and mobile subscriptions exceeded 65 million, according to the Communications Authority of Kenya. This surge in digital access has led to numerous benefits, such as improved financial services, enhanced government service delivery, and new business opportunities [6]. However, the country’s rapid digitalization also presents new challenges, particularly in protecting critical infrastructure and sensitive data from cyber threats. Cyberattacks could potentially disrupt key sectors such as healthcare, education, and finance, ultimately harming the economy and impeding the country’s development goals [6].

One area of growing concern is the vulnerability of county government ICT systems. The Kenya National Bureau of Statistics reported a staggering KES 29.5 billion (USD 230 million) lost to cybercrime in 2022, signaling the need for urgent intervention. County governments, often with limited resources and outdated technology, are increasingly targeted by cybercriminals. These vulnerabilities expose critical public services and sensitive citizen data to exploitation, resulting in potential breaches of privacy, financial losses, and even the interruption of essential services. To mitigate these risks, it is crucial for local governments to adopt stronger cybersecurity tools, practices, and technologies to safeguard against such threats and ensure the continuity of public services [6].

Tackling Kenya's cybersecurity challenges requires a collaborative approach involving the government, private sector, and international partners. Key initiatives include creating a comprehensive national cybersecurity strategy aligned with global best practices to address local challenges, investing in education and training programs to bridge the cybersecurity skills gap, fostering public-private partnerships for sharing threat intelligence and best practices, and strengthening regulatory frameworks and enforcement to ensure compliance with cybersecurity standards across all sectors[6].

The Kenyan government has responded to cyber threats by integrating control measures into its national information security strategy, aligned with Kenya's Vision 2030.[7] The Ministry of ICT's National Cyber Security Strategy outlines the government's mandate, key goals, and funding for relevant laws, and promotes technological advancement in computer hardware and software[7],[9]. This strategy emphasizes the protection of national information security and stakeholders, and acknowledges the need for collaboration with local government, the private sector, academia, and other agencies. Kenya aims to become a leading partner in cybersecurity in Africa and globally [7],[9].

Reports indicate that major cybersecurity issues in Kenya often lack strategies for effective cyberattack control and mitigation [8]. Additionally, relevant sectors frequently lack implementation strategies to address

identified system weaknesses. Kenya's cybersecurity vision and objectives primarily emphasize security and infrastructure, but the national strategy has limitations, as it does not sufficiently address other critical factors, including cybersecurity awareness, policies and regulations, and funding [8],[9].

The growth of technology, including the 2009 installation of fiber-optic cables in the East African Community, has driven ICT growth[8], [9] . However, the rapid evolution of cyberattacks, outpacing the development of cyber defenses, has led to an increase in their frequency. Cyberattacks, which have grown in complexity since the 1980s, are perpetrated by various actors, including hacktivists, cybercriminals, cyber-terrorists, and those with national security agendas. These attacks, ranging from basic internal breaches to sophisticated external intrusions, pose significant threats and risks that require a comprehensive cybersecurity strategy [8], [9].

The 2014 Kenya National Cyber Security Strategy report highlights the increasing cybersecurity challenges due to rapidly evolving technologies. The report emphasizes the need for proactive measures to control cybercrime, promote economic growth, and safeguard information systems[10]. The Kenyan government acknowledges the risks of emerging cyber threats and the necessity of addressing them to enable technological advancement and economic development. The report also acknowledges that technological advancements, while enhancing global information access, also create vulnerabilities that can be exploited by attackers. Kenya's National Cyber Security Master Plan is designed to manage these cyberattack risks and address emerging threats to the ICT sector [10].

The 2014 cybersecurity report had certain gaps. It does not clearly articulate how its initiatives will effectively control attacks [10], [11], and it inadequately addresses critical areas of cyber defense. This gaps have since been addressed by the revised report of 2024 where A comprehensive cybersecurity strategy encompassing technology infrastructure and security has been factored, in addition policies and regulations, implementation strategies, the development of cybersecurity expertise, adequate funding, and public awareness education are addressed. Furthermore, the report partially address the specific cyber risk challenges affecting Kenyan systems [10], [11]

III. Effects Of Cybersecurity

The integration of ICT systems within Kenyan county governments has revolutionized operations, enhancing efficiency and service delivery. However, this digital transformation has also exposed these systems to increased cybersecurity vulnerabilities, with potentially severe consequences. Successful cyberattacks can disrupt essential services, compromise sensitive data, and lead to significant financial losses. For instance, attacks targeting critical infrastructure like financial management systems can impede service delivery, delay employee salaries, and disrupt crucial economic functions within the county[11], [12].

Moreover, weak cybersecurity can erode public trust and hinder the adoption of digital services. Citizens are less likely to engage with online platforms for services such as tax payments, permit applications, or accessing public information if they fear their data is insecure. This can undermine efforts to improve transparency, accountability, and citizen participation in governance. The reputational damage from successful cyberattacks can also have long-lasting effects on a county government's ability to attract investment and partner with other organizations[11], [12].

To mitigate these risks, county governments must prioritize robust cybersecurity measures. This includes implementing strong security policies, investing in up-to-date security technologies, and providing regular training for staff and citizens on cybersecurity best practices. Failure to address cybersecurity comprehensively can lead to a vicious cycle of increased attacks, loss of trust, and hindered development, ultimately undermining the potential of ICT systems to improve governance and service delivery in Kenya's counties[11], [12].

The interconnected nature of modern ICT systems means that a single point of failure can have cascading effects across multiple county departments and services. For example, a ransomware attack on a county's network could cripple not only its internal operations but also its ability to deliver essential services to citizens, such as healthcare, emergency response, and utilities management. This disruption can have profound social and economic consequences, particularly for vulnerable populations who rely heavily on these services[11], [12].

Furthermore, the evolving threat landscape presents a continuous challenge for county governments. Cybercriminals are constantly developing new and more sophisticated attack methods, making it difficult for even well-resourced organizations to stay ahead. This necessitates a proactive and adaptive approach to cybersecurity, with ongoing monitoring, threat intelligence gathering, and regular updates to security systems. County governments must also foster collaboration and information sharing with other government agencies, the private sector, and international partners to effectively address the complex and evolving nature of cyber threats[11], [12].

IV. Related Literature

County governments and stakeholders must prioritize cybersecurity challenges and risks. The proliferation of high-speed internet has transformed organizational operations, increasing efficiency but also introducing significant cyberattack vulnerabilities. To effectively manage these escalating vulnerabilities, rigorous research into cybersecurity vulnerability attacks is essential.

Previous research, such as that by [13], has explored relevant cybersecurity models. A cybersecurity model can be defined as a framework that describes how a cybersecurity system functions, incorporating measurement tools to assess the current cybersecurity posture, and strategies to strengthen defenses or prevent future exploitation of weaknesses. This approach enables organizations to understand and improve their security standing[13].

A maturity model is a structured framework that shows how an organization's abilities in a specific area grow over time, like going from "Crawl" to "Walk" to "Run." It helps organizations see where they currently stand (benchmark) and figure out what they need to improve and focus on to reach their goals. For example, the C2M2 helps organizations measure and improve their cybersecurity over time by setting target levels based on risk and planning how to get there.

According to [16], "maturity" implies evolutionary progress in the demonstration of a specific ability or in the accomplishment of a target from an initial to a desired or normally occurring end stage. The concept of maturity has proven to be useful in the study of the development of organisations and their processes and has been applied through various maturity models [14], [15], [16]. As summarised in, maturity models divide evolutionary progress into a sequence of levels or stages that form a logical path from an initial state to a final level of maturity. These levels and stages are used to derive and prioritise improvement measures and control the progress of change.

Maturity models therefore provide information about a company's current status and how to improve it. They offer a simple but effective tool to measure organisations' capabilities and contribute to transformation and the development of competencies in an organisation by initiating a change process. The maturity models can also be used as benchmarking tools to compare organisations with each other to set development goals, or as self-review frames and managerial tools for self-improvement action [14], [15], [16].

Maturity models are therefore a widely used tool in evaluating certain aspects of organisations, since they represent an increasingly organised and systematic way to do business . Moreover, they can also be used in developing an organisation's future vision and path. In accordance with this, has identified three different purposes for developing a maturity model: descriptive, comparative, and prescriptive[14], [15], [16] . Maturity models serve a descriptive purpose when they are used for 'as-is' assessments to evaluate the current capabilities of the organisation, usually according to specific criteria. A comparative purpose enables internal or external benchmarking and comparison of similar business units and organisations, while a prescriptive purpose is to indicate how to determine desirable maturity levels and provide guidance for improvement actions[14], [15], [16].

This analysis emphasizes the application of existing maturity models and initiatives to address the identified problems. Cybersecurity maturity models are crucial for organizations aiming to develop and refine their processes to achieve a higher state of cybersecurity readiness. These models offer a structured approach to gaining control over cybersecurity, aiding in the development of robust security programs and processes that enable organizations to proactively prevent, detect, respond to, and recover from cyber incidents. Organizations must first assess their current cybersecurity preparedness to establish a roadmap for improvement [14], [15], [16].

Several key maturity models are relevant in this context, Cybersecurity Capability Maturity Model (C2M2): This model, particularly versions developed by the U.S. Department of Energy (DOE), provides a framework for evaluating and enhancing an organization's cybersecurity capabilities, especially in critical sectors like energy. It helps organizations measure their progress over time and prioritize security investments, Community Cybersecurity Maturity Model: This model helps communities, including local government entities, assess and improve their cybersecurity posture. It's tailored to the unique challenges and resource constraints often faced by these entities, Cybersecurity Culture Maturity Model: This model focuses on the human element of cybersecurity, recognizing that a strong security culture is essential for effective cyber defense. It provides guidance on how to cultivate a workforce that is aware of security risks and actively participates in protecting organizational assets, Security Assessment Model Initiatives in Africa: Various initiatives across Africa aim to improve cybersecurity assessment practices. These are crucial for understanding the specific challenges and needs of organizations within the African context and for developing tailored solutions. Examples include efforts to harmonize cybersecurity standards and build local expertise, NIST Cybersecurity Framework (CSF) Maturity Levels: The National Institute of Standards and Technology (NIST) provides a framework with maturity levels (Partial, Risk-Informed, Repeatable, and Adaptive) that organizations can use to assess and improve their cybersecurity posture. This framework is widely recognized and used globally, Cybersecurity Maturity Model Certification (CMMC): This model, developed by the U.S. Department of Defense (DoD), is designed to protect sensitive information within the defense industrial base. While initially focused on defense contractors, its

principles offer valuable lessons for any organization seeking to enhance its cybersecurity maturity [14], [15], [16].

Maturity models offer numerous benefits, including, Structured Improvement: They provide a structured path for organizations to enhance their cybersecurity capabilities over time, Benchmarking [19]: They allow organizations to benchmark their current practices against industry standards and best practices, Risk Management: They help organizations identify and prioritize cybersecurity risks, enabling them to allocate resources effectively, Roadmap Development: They assist in developing a roadmap for implementing security improvements and achieving desired maturity levels, Effective Communication: They provide a common language and framework for communicating about cybersecurity within the organization and with external stakeholders[19].

V. Methodology

A comprehensive review of existing literature was undertaken, drawing from academic publications, industry reports, government documents, and news articles to explore the impact of cybersecurity vulnerabilities on ICT systems in Kenyan county governments. This desktop research provided valuable insights into the current cybersecurity landscape, highlighting key challenges and emerging threats. It also enabled a comparison of Kenya's cybersecurity risk environment with global trends, helping to contextualize the country's position within the broader international framework.

VI. Recommendations

The integration of ICT systems in Kenyan county governments has improved efficiency but increased cybersecurity vulnerabilities, leading to potential disruptions of essential services, data compromise, and financial losses; weak cybersecurity can erode public trust, hinder digital service adoption, and damage a county's reputation, necessitating robust measures like strong policies, investment in security technologies, staff and citizen training, incident response plans, and enhanced collaboration to mitigate risks and ensure the effective use of ICT for governance and service delivery.

VII. Conclusions

The adoption of ICT systems by Kenyan county governments has significantly enhanced operational efficiency, but it has also increased their exposure to cybersecurity threats. These vulnerabilities can result in service disruptions, data breaches, and financial losses. Without adequate cybersecurity measures, public confidence may be eroded, digital service uptake could decline, and the counties' reputations may suffer. To fully leverage ICT for effective governance and service delivery, it is essential for county governments to implement comprehensive security measures. This involves establishing clear policies, investing in modern security technologies, training both staff and the public, preparing incident response plans, and encouraging collaborative efforts. In summary, while ICT offers substantial benefits to county-level governance, these can only be fully realized if cybersecurity risks are addressed through a well-structured and unified approach.

References

[1] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, And E. Akin, "A Comprehensive Review Of Cyber Security Vulnerabilities, Threats, Attacks, And Solutions," Electronics, Vol. 12, No. 6, Pp. 1–42, Mar. 2023, Doi: Https://Doi.Org/10.3390/Electronics12061333.

[2] X. Liu Et Al., "Cyber Security Threats: A Never-Ending Challenge For E-Commerce," Frontiers In Psychology, Vol. 13, No. 6, Apr. 2022, Doi: Https://Doi.Org/10.3389/Fpsyg.2022.927398.

[3] J. A. Blackley, T. R. Peltier, And J. Peltier, Information Security Fundamentals. Auerbach Publications, 2004. Doi: Https://Doi.Org/10.1201/9780203488652.

[4] M. Abu And R. Nath, "Navigating The Cyber Security Landscape: A Comprehensive Review Of Cyber-Attacks, Emerging Trends, And...," Researchgate, Feb. 21, 2024. Https://Www.Researchgate.Net/Publication/378343830_Navigating_The_Cyber_Security_Landscape_A_Comprehensive_Review_Of_Cyber-Attacks_Emerging_Trends_And_Recent_Developments (Accessed Apr. 17, 2025).

[5] Cak -National Ke-Cirt/Cc, "Cybersecurity Report 2024 36th Edition - Cyber Threat Landscape Overview," National Ke-Cirt/Cc, Nairobi - Kenya, Dec. 2024. Accessed: Apr. 17, 2025. [Online]. Available: Https://Ke-Cirt.Go.Ke/Wp-Content/Uploads/2025/01/2024-25-Q2-Cyber-Security-Report.Pdf

[6] Csm, "Cybersecurity Is A Legitimate Threat To Kenya's Digital Future," Rising Cases Trigger Cybersecurity Concerns, Oct. 05, 2024. Https://Www.Csm.Tech/Africa/Blog-Details/Cybersecurity-Is-A-Legitimate-Threat-To-Kenyas-Digital-Future (Accessed Apr. 17, 2025).

[7] R. Of K. Lane, "The Republic Of Kenya Draft Kenya Cybersecurity Strategy, 2025 -2029 National Computer And Cybercrimes Coordination Committee (Nc4) Herufi House, 2nd Floor," Republic Of Kenya, Nairobi , Kenya, Apr. 2025. Accessed: Apr. 23, 2025. [Online]. Available: Https://Nc4.Go.Ke/Storage/2025/03/National-Cybersecurity-Strategy-2025-2029-Draft.Pdf

[8] M. Kabaya And M. Kageni, "Cyber Security In The Wake Of The Fourth Industrial Revolution In Kenya," Kippra, Nairobi , Kenya, Jun. 2024. Accessed: Apr. 23, 2025. [Online]. Available: Https://Yp-Alumni.Kippra.Or.Ke/Wp-Content/Uploads/2024/10/Dp326.Pdf

[9] The National Ke-Cirt/Cc, "Cybersecurity Report 31 St," May 2023. Accessed: Apr. 23, 2025. [Online]. Available: Https://Www.Ca.Go.Ke/Sites/Default/Files/2023-10/Cybersecurity%20report%20q1%202023-2024.Pdf

[10] Serianu, "Kenya Cyber Security Report 2014 Rethinking Cyber Security - 'An Integrated Approach: Processes, Intelligence And Monitoring.,'" Serianu, Apr. 2022. Accessed: Apr. 23, 2025. [Online]. Available: Https://Www.Serianu.Com/Downloads/Kenyacybersecurityreport2014.Pdf

[11] National Defense University -Kenya, "Values," Jndu-K, Nairobi , Kenya, Mar. 2024. Accessed: Apr. 23, 2025. [Online]. Available: Https://Ndu.Ac.Ke/Sites/Default/Files/2024-10/The%20national%20security%20journal%20volume%202%20issue%201%20%282024%29.Pdf

[12] A. Aliyu Et Al., "A Holistic Cybersecurity Maturity Assessment Framework For Higher Education Institutions In The United Kingdom," Applied Sciences, Vol. 10, No. 10, P. 3660, May 2020, Doi: Https://Doi.Org/10.3390/App10103660.

[13] A. Brezavšček And A. Baggia, "Recent Trends In Information And Cyber Security Maturity Assessment: A Systematic Literature Review," Systems, Vol. 13, No. 1, P. 52, Jan. 2025, Doi: Https://Doi.Org/10.3390/Systems13010052.

[14] D. P. Dube And R. P. Mohanty, "Towards Development Of A Cyber Security Capability Maturity Model," International Journal Of Business Information Systems, Vol. 34, No. 1, P. 104, Feb. 2020, Doi: Https://Doi.Org/10.1504/Ijbis.2020.106800.

[15] G. Lee, S. Kim, I. Lee, S. Brown, And Y. A. Carbajal, "Adapting Cybersecurity Maturity Models For Resource-Constrained Settings: A Case Study Of Peru," The Electronic Journal Of Information Systems In Developing Countries, Vol. 5, No. 2, Oct. 2024, Doi: Https://Doi.Org/10.1002/Isd2.12350.

[16] Office Of Cybersecurity, Energy Security, And Emergency Response, "Cybersecurity Capability Maturity Model (C2m2)," Energy.Gov, Jun. 01, 2022. Https://Www.Energy.Gov/Ceser/Cybersecurity-Capability-Maturity-Model-C2m2 (Accessed Apr. 23, 2025).