REVIEWED JOURNAL of INTERNATIONAL SOCIAL SCIENCE & HUMANITIES
[ISSN 2663-127X]

Vol. 5, Iss. 1 (2024), pp 463 – 480, October 11, 2024. www.reviewedjournals.com, ©Reviewed Journals

EVALUATING CYBERSECURITY THREATS, MEASURES, AND EFFECTIVE FACTORS FOR ENHANCING THE SECURITY OF KENYA'S ECITIZEN PLATFORM

[1] Jennifer Chebet Sitienei & [2] Dr. John Kandiri, PhD

[1] Master of Arts in Security Management and Police Studies, School of Law, Arts and Social Sciences, Kenyatta University, Kenya

[2] Senior Lecturer, Department of Computing and Information Science, Kenyatta University, Kenya

Accepted: September 18, 2024

ABSTRACT

This research explored the cybersecurity environment of Kenya's eCitizen platform, a crucial tool for accessing government services in the face of rising global cyber threats. The study focused on protecting sensitive governmental data, with objectives that included analyzing cybersecurity threats, evaluating mitigation strategies, and providing actionable recommendations. The literature review thoroughly examined each objective through the lens of established cybersecurity models such as Defense in Depth, Zero Trust, and the Integrated Theory of Cybercrimes. These models offered proactive strategies and comprehensive frameworks for strengthening cybersecurity defenses. In terms of methodology, the research utilized a descriptive research design with a case study approach and stratified sampling technique to systematically investigate cybersecurity threats and management strategies specific to the eCitizen platform. This approach enabled a detailed examination of the unique challenges and solutions related to cybersecurity within this context. The analysis incorporated regression analysis to quantify the relationships between cybersecurity threats, mitigation measures, and the effectiveness of these measures in enhancing the security of the eCitizen platform. The regression model revealed that predictors such as cybersecurity threats, security measures, and effectiveness factors are significantly correlated with the platform's security effectiveness. This statistical analysis highlighted key areas where improvements could be made and provided a data-driven basis for recommendations. The discussion critically evaluated the impact of cybersecurity threats and digitalization trends in Kenya, addressing issues such as demographic factors, challenges in managing cyber threats, and the perceived effectiveness of various security measures. The conclusions emphasized the need for improved governance, enhanced risk management practices, updated legislation, and increased international cooperation to address evolving cyber threats effectively. The study also recommended further research to align with global cybersecurity best practices, aiming to enhance resilience and public trust in online government services. Overall, this research contributed significantly to understanding the cybersecurity challenges faced by Kenya's government services, advocating for proactive measures, transparent communication, and collaborative efforts across sectors to improve security and public confidence in digital services.

Key Words: *System Security, Cyber Attack, Digitization, E-citizen, Kenya*

CITATION: Sitienei, J. C., & Kandiri, J. (2024). Evaluating cybersecurity threats, measures, and effective factors for enhancing the security of Kenya's E-citizen platform. *Reviewed Journal of Social Science & Humanities*, 5 (1), 463 – 480.

INTRODUCTION

Advancements in technology have revolutionized how governments offer services to their citizens. Today, government services are increasingly becoming accessible through various digital platforms. For example, there is GOV.UK for the United Kingdom, e-Estonia for Estonia, Aadhaar, Digi Locker and UMANG for India, Sing Pass for Singapore, GEA portal for Saudi Arabia, Irembo for Rwanda, and ECitizen for Kenya. Buckland et al. (2015) pointed out that the adoption of digital government services by countries brings about various advantages to the citizens, businesses, and the government at large. These advantages cut across the mitigation of corruption, enhancement of service provision, convenience, accessibility, and efficiency to the public. Milakovich, M. E. (2012) further notes that the platform offers 24/7 availability, saving time and reducing costs for citizens and the government. This means that online services increase access, transparency, and environmental sustainability while streamlining processes and improving accountability. Nonetheless, this shift has been observed to concurrently introduce fresh susceptibilities to cyber threats. According to (Khaemba et al., 2017) exploiting technology, criminals target online users, leading to financial setbacks and compromises in privacy

The rapid advancement of technology and the increasing reliance on digital platforms have led to a significant increase in cybercrimes worldwide, as highlighted by Ecclesiastical (2020), Świątkowska (2020), and Benard et al. (2021). This growing trend poses a major threat to data privacy, security, and the overall well-being of internet users, affecting individuals, businesses, and governments alike. According to a report by Malik, J. K., & Choudhury, S. (2019), the increasing sophistication of technology is cited as the primary driver behind the surge in cybercrimes. The report emphasizes that cybercriminals capitalize on vulnerabilities within evolving technologies to illicitly obtain personal information. Moreover, the interconnected nature of devices, such as the Internet of Things (IoT), is highlighted as a factor that expands the attack surface for cybercriminals, thereby simplifying their ability to target both individuals and organizations. This is evident with the online government services.

Mahlangu and Ruhode (2021) pointed out that the increasing digitization of government services and storage of sensitive citizen data in digital databases have made governments vulnerable to cyber-attacks. For instance, in 2015 US Office of Personnel Management (OPM) suffered a major breach where the sensitive personal information of millions of federal employees and contractors was compromised. Likewise, in 2027 United Kingdom government also faced cyber-attacks targeting its digital infrastructure where the WannaCry ransomware attack disrupted the operations of the National Health Service (NHS) leading to the cancellation of appointments and the postponement of surgeries.

Suleiman et al. (2020) define cybercrimes as an illegal activity where a computer interface or content structure is either a resource a target, or a combination of both. Consequently, Shankar, Hemarj, and Panda (2021) describe cybersecurity threats as e-offenses, computer-related offenses, elevation development crime, and digital age crime. Further Vinayak Pujari, Dr. R. B. Patil (2020) defined it as a crime arising outside electronic messages or computer systems.

The surge in cyber-attacks was attributed to the widespread adoption of remote working systems and increased online activity when most businesses and organizations moved to remote work environments as was seen during the Covid-19 Pandemic. At such time cyber criminals exploit vulnerabilities in misaligned networks and unsecured home devices. According to reports by Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022), cyberattacks increased by 58% globally in 2020 compared to 2019 and the trend continued in 2021, with cyberattacks increasing by 125% by the end of the year. This highlights the importance of organizations and individuals taking proactive measures to secure their networks and devices to protect against cyber threats. individuals should also practice good cybersecurity hygiene by using strong passwords, keeping software up to date, and being cautious of suspicious emails or links.

It is worth noting that government websites are particularly vulnerable, experiencing a 47% increase in internet attacks. This highlights the urgent need for enhanced cybersecurity measures to protect critical infrastructure and sensitive data.

ECitizen, the Kenyan e-government platform was launched in 2014, and revolutionized access to government services by enabling citizens to conveniently interact with various governmental functions online. Before its introduction, citizens had to navigate complex bureaucratic processes, endure long queues, and make multiple visits to various government offices to obtain necessary documents or complete transactions. This often led to inefficiencies, delays, and opportunities for corruption.

As of March 2024, the platform has onboarded over 5000 services that citizens can access. This means that citizens and businesses can now access various services all from the comfort of their homes or offices. Despite its significant benefits, the ECitizen platform faces numerous cyber threats due to the nature of the data it handles. The platform receives, processes stores, and transmits voluminous personal data of different agencies. These vulnerabilities expose the platform to malicious activities such as data breaches, denial of service, phishing attempts, and malware incidents(Muthengi, 2015). The vulnerabilities within the ECitizen platform present significant risks to the security and integrity of the system. With its extensive collection of sensitive personal and financial data, the platform becomes a prime target for cybercriminals seeking to exploit weaknesses in its defenses. From phishing attacks aimed at deceiving users into divulging their credentials to insider threats posed by employees with privileged access, the platform faces multifaceted risks. Additionally, the reliance on weak authentication methods and the potential for supply chain attacks further exacerbate these vulnerabilities. Without robust security measures in place, such as encryption, regular security audits, and user education on cybersecurity best practices, the ECitizen platform remains susceptible to data breaches, malware infections, and service disruptions (Muthengi, 2015). Addressing these vulnerabilities requires a comprehensive approach that encompasses technical controls, employee training, and proactive monitoring to mitigate emerging threats and safeguard the platform's users and their data.

Statement of the Problem

The increasing use of digital technology in government has led to concerns about keeping information safe and protecting people's privacy. When governments gather, store, and share citizen data, their wish is that the data is secure and not misused, especially with the growing risk of cyberattacks. The fact remains that as governments offer more services online, they become more at risk from cyber criminals who want to exploit weaknesses in their systems, which could lead to data theft, financial fraud, service disruptions, and even threaten national security Serianu (2019).

In the digital age, citizens worry about privacy and a lack of trust that is making it harder for e-government initiatives to succeed. Previous research shows that when individuals feel like their privacy is being invaded, they start to doubt and mistrust the government. This privacy problem happens when one's intention is to keep personal information private as they share the information online and with no knowledge of the risks of using digital technology. In line with Kahlil Gibran's insight, which notes that; “if one divulges their secrets to the wind, they cannot hold the wind accountable for sharing them with the trees”.

Therefore, this study aims to comprehensively analyze the diverse array of cyber threats targeting the eCitizen platform, evaluate the existing strategies employed to mitigate cybercrimes and scrutinize the cybersecurity governance framework influencing these strategies.

The purpose of the study.

The primary purpose of the study is to investigate the cyber security framework governing the eCitizen platform in Kenya. The study was guided by the following specific objectives:

- To identify forms of cyber security threats on the eCitizen platform in Kenya

- To establish the cyber security measures employed to mitigate cyber security threats on the eCitizen platform in Kenya
- To determine the factors affecting the effectiveness of the measures put to manage the cybersecurity threats on eCitizen platform
- To provide recommendations for enhancing resilience to cyber threats, improving incident response capabilities, and strengthening overall cybersecurity posture.

LITERATURE REVIEW

Everyday governments, citizens and businesses increasingly depend on technology to oversee their functions, ranging from Government to Government (G2G) Government to Citizens (G2C) operations, Government to Business (B2B) and Business to Business (B2B) (Cho et al., 2022) This over reliance on technology is leading to the convergence of various technological platforms, tools, and interfaces, all interconnected through an internet that is swiftly transitioning to a more decentralized version (Schroers & Tsormpatzoudi, 2016). This occurrence also brings about a more intricate cyber threat landscape, along with an increasing number of vulnerable points of data privacy issues. (Oseni et al., 2015) notes that as society continues migrating to digital arena the looming threat of cybercrime becomes more pronounced, often resulting in substantial financial losses and trust issues.

Kenya is among those countries that is experiencing a growing number of threats in cyberspace that threaten Information, Communications and Technology (ICT), infrastructure as well as citizens' privacy and eventually national security. In 2022 survey by Cyber Security Team on the experience on cybersecurity threats, Kenya was ranked fourth in Africa, after Algeria, Egypt and South Africa. The report stated that criminals, have found a way of using computers and the internet to get into organizational websites, personal accounts and emails with the aim of getting the data.

Manjula et al., (2023) discusses hacking as another pertinent threat, where unauthorized access is gained to computer systems. Further noted the motivations behind hacking has ranged from curiosity to seeking sensitive data or fulfilling an agenda. Aaccording to Denning, D. E. (2019) hacktivist is driven by social or political activism which poses a cybersecurity threat to government organizations responsible for shaping and enforcing laws and policies. Government institutions which is regarded as symbols of authority and control can become targets for hacktivists aiming to challenge specific governmental actions and values (Goode, L. 2018). Moreover, Smith and Jamieson (2023) emphasize email bombing and spamming as another cybersecurity threats activities that overwhelm recipients' systems with excessive emails, potentially causing server crashes. They note that spamming, in particular, involves sending unsolicited bulk messages, often for advertising purposes.

Data encryption practices are now being widely adopted by various organizations as a proactive measure to safeguard their sensitive information, as highlighted in the study by Oseni et al. (2015). It has been emphasized that storing data in plain text format exposes it to vulnerabilities, making it susceptible to unauthorized access by malicious actors. Cho et al. (2022) further elaborate that data encryption plays a crucial role in restricting data access solely to authorized parties possessing the encryption key, thereby ensuring that even if unauthorized entities manage to breach the security measures, they are unable to decipher the encrypted data. Moreover, many organizations utilize sophisticated data encryption software solutions that not only enable them to detect any unauthorized attempts to modify or compromise the data but also provide real-time alerts in case of any suspicious activities.

The utilization of firewalls, data encryption, intrusion detection systems, and access controls has been empirically validated as an effective approach to enhancing the security posture of online government websites, as highlighted in the publication "Cybersecurity Trends in Government" from the year 2023. These multifaceted measures play a crucial role in the regulation of traffic flow, identification of unauthorized access attempts, and restriction of user permissions based on specific job functions, thereby significantly strengthening the platform's defenses against a wide range of cyber-attacks that may pose threats to the integrity and confidentiality of sensitive government information. Moreover, employee education and awareness initiatives are underscored as pivotal components within the realm of cybersecurity strategies designed for online government websites. The implementation of comprehensive training programs serves the purpose of equipping government personnel with the necessary knowledge and skills pertaining to cybersecurity best practices, thereby empowering them to effectively recognize and mitigate potential cyber threats that may compromise the security and functionality of the government's online platforms. Nevertheless, despite the diligent implementation of these security measures and educational initiatives, instances of security breaches may still transpire, thereby emphasizing the imperative need for a continuous cycle of adaptation and enhancement in the domain of cybersecurity protocols. By closely adhering to the recommendations delineated in the latest cybersecurity reports, online government websites can effectively enhance their resilience against evolving cyber threats, consequently ensuring the robust protection of citizen data and the uninterrupted delivery of essential government services to the public.

The Cybersecurity and Infrastructure Security Agency (CISA) offers comprehensive recommendations aimed at enhancing patch management practices and mitigating associated risks (CISA, 2022). Statistics reveal that over 60% of breaches are linked to vulnerabilities for which a patch was available but not applied.

Proactive threat intelligence gathering and timely updates to security controls are deemed essential for countering evolving cyber threats (European Union Agency for Cybersecurity, 2023). Statistics reveal that cyber attacks targeting government entities have increased by over 50% in the past year alone. The National Cyber Security Centre (NCSC) provides insights and recommendations on cybersecurity governance tailored for government entities (NCSC, 2022). Studies indicate that organizations with effective cybersecurity governance structures experience 60% fewer security incidents compared to those without.

Defense in Depth Theory

The Defense in Depth theory, as articulated by Smith (2022) and further conceptualized by Coole & Brooks (2011), is a foundational security approach aimed at protecting assets in the context of preventing theft, destruction of facilities, and ensuring the well-being of personnel and information. This theory emphasizes the implementation of multiple layers of security barriers to impede unauthorized access and provide opportunities for an appropriate response and recovery in the event of a security breach. In the realm of cybersecurity threats, the Defense in Depth approach is highly relevant and effective. Just as physical assets and facilities require multiple layers of protection, digital assets and systems also benefit from a layered security strategy.

The theory suggests using multiple layers of security to protect against cyber threats, like hackers or malware. This means not relying on just one security measure, but having many different ones in place. For example, to deter attackers one might use passwords or encryption. Detection tools, like antivirus software, help spot when something suspicious is happening. Delay tactics, such as firewalls, slow down attackers if they do get in. And if there is a breach, response and recovery plans help to fix the problem and get things back to normal. This approach is like having several locks on your door instead of just one. It makes it harder for attackers to get in and cause damage. Plus, it's important to look at the bigger picture and understand how all the security measures work together to keep things safe.

Zero Trust Theory

The Zero Trust approach to cybersecurity, pioneered by John Kindervag in 2009 explains a paradigm shift in how organizations approach security. It challenges the traditional notion of implicit trust and advocates for a "Never Trust, Always Verify" philosophy. In the face of evolving cyber threats originating from both internal and external sources, Zero Trust Architecture (ZTA) recognizes that the traditional perimeter-based security model is no longer sufficient.

At the core of ZTA are principles such as identity verification, least privilege access, and continuous monitoring. By leveraging technologies like multi-factor authentication (MFA), identity and access management (IAM), and micro-segmentation, ZTA aims to ensure that only authenticated users and devices can access specific resources, and that access is granted based on the principle of least privilege, limiting users' access to only the information necessary for their roles. This granular approach to access control minimizes the potential attack surface and enhances security. By embracing ZTA principles and integrating Layered Security, organizations can enhance their resilience against evolving cyber threats and safeguard critical assets effectively in an increasingly complex threat landscape.

Integrated Theory

The Integrated Theory of Cybercrimes amalgamates various criminological perspectives, such as Routine Activity Theory (RAT), rational choice theory, and social learning theory, to furnish a comprehensive comprehension of cyber criminal conduct. Developed and expounded upon by Thomas J. Holt and fellow criminologists, this theory furnishes a holistic approach to managing cybercrimes on online government portals. By considering individual incentives, organizational dynamics, and environmental influences, the theory aids in identifying and addressing the root causes contributing to cybercrimes. Its aim is to propose measures for risk mitigation and enhance the security of government portals, thereby fostering a safer online environment.

By combining various criminological perspectives, the Integrated Theory of Cybercrimes provides a comprehensive framework for elucidating and managing cybercrimes efficaciously. It encompasses individual incentives, organizational dynamics, and environmental circumstances that shape cyber-criminal behaviour.

Conceptual Framework

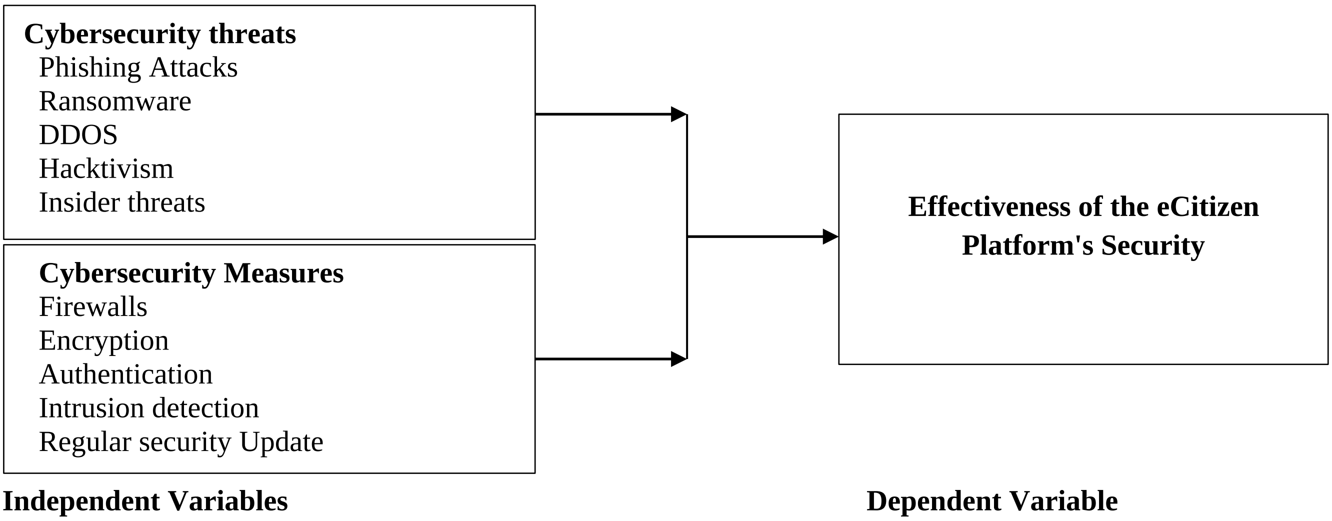

Figure 1: Conceptual Framework

METHODOLOGY

The study used a descriptive research design and both qualitative and quantitative data were gathered. This study is centered on the eCitizen platform, which stands as the predominant online gateway for accessing government services in Kenya.

The study on cyber security threats on the ECitizen platform in Kenya targeted a diverse group of individuals. This included individual users of the eCitizen platform who actively engage with the platform, such as front users and end users accessing government services and documents. Additionally, it encompassed government personnel responsible for managing and safeguarding the platform, such as IT professionals, administrators, and policymakers. Experts in cyber security, particularly those familiar with the ECitizen platform or similar online government services, were also part of the target population to provide insights into potential threats and vulnerabilities. Moreover, Information and Communication Technology (ICT) professionals involved in developing, maintaining, or auditing online government platforms were included. Lastly, individuals or organizations advocating for digital rights, online privacy, and cyber security awareness were sought to offer valuable perspectives on the subject matter.

The research study utilized a stratified sampling technique. The validity of the questionnaire was ensured by designing it to accurately measure the respondents' knowledge and understanding of cybercrimes and their management through the ECitizen portal in Kenya.

Quantitative information gathered in this study was processed descriptively supported by means and standard deviations. These were reinforced by inferential tools especially regression analysis. The software that played a role during analysis of the findings was the SPSS.

FINDINGS

Response Rate

Out of the 204 questionnaires administered, 184 were returned and deemed suitable for analysis. The study's response rate of 92% is commendable, exceeding the recommended 70% response rate for social studies research.

Table 1: Response Rate

Response	Number	Percentage
Responded	184	91%
Not Responded	20	9%
Total	**204**	**100**

Author data, 2024

Cybercrimes Threat Awareness

The study sought to assess the level of cybersecurity awareness among the respondents. The findings are shown below.

Table 2: Cybersecurity Threats Awareness

Response	Number	Percentage
YES	145	78.8
NO	39	21.2
Total	**184**	**100**

The findings indicate that a substantial majority of respondents (78.8%) reported being aware of cybersecurity threats. This high level of awareness suggests that most professionals in the field have a fundamental understanding of cybersecurity concepts and potential threats. This is critical for effective cybersecurity practices, as awareness is the first step in identifying and mitigating cyber risks. This suggests that most individuals in the field understand the importance of cybersecurity and are likely to engage in practices that protect their organizations from cyber threats.

However, 21.2% of respondents indicated a lack of awareness. This highlights a significant area for improvement. Enhancing cybersecurity awareness among this group is essential to ensure that all members of the organization are equipped to recognize and respond to cyber threats.

Most research supports the notion that high levels of cybersecurity awareness are crucial for effective cybersecurity practices. Awareness helps in the early identification of potential threats and the implementation of appropriate mitigation strategies (Smith, 2020). Furthermore, targeted training programs have been shown to significantly improve cybersecurity awareness and preparedness among employees (Jones & Ashenden, 2019). Continuous education is necessary to keep pace with the evolving landscape of cyber threats (Williams, 2018).

Forms of Cybersecurity Threats

The participants were asked to assess the prevalence of various cybersecurity threats in their organization on a scale of 1 to 4 where 1 = Never, 2= Not Sure, 4= Rare, and 4 = Frequent. The mean and standard deviation were computed to aid in the comprehension and extrapolation of the results. The findings are shown in the Table below.

Table 3: Forms of cybersecurity threats to eCitizen platform in Kenya

Cybersecurity Threats	Mean	Median	Std. Deviation
Denial of Service	3.08	3	0.859
Malicious Software's.	3.16	3	0.872
Insider Threats	2.51	2	0.761
Cyber Stalking	2.35	2	1.246
Hacking	3.39	3	0.668
Phishing.	3.65	4	0.731
Data breaches	1.65	2	0.692
Identity fraud	2.83	3	0.88

The data collected from the study on prevalent cybersecurity threats on the eCitizen platform in Kenya revealed a range of perceived threat levels. The mean values provided an average assessment of each threat category's severity, with higher mean scores indicating a greater perceived threat. Denial of Service (DoS) attacks were reported as moderately severe, with a mean score of 3.08. This value, slightly above 3, suggested that respondents viewed DoS attacks as significant but not the most critical threat. The median of 3 supported this view, reflecting general agreement on its moderate severity. The standard deviation of 0.859 indicated some variability in perceptions. This aligns with previous studies, which have noted that while DoS attacks can be disruptive, their perceived severity may vary depending on the context and impact on services (Shin et al., 2020; Kshetri, 2021).

Malicious software was perceived as similarly severe to DoS attacks, with a mean rating of 3.16. The median of 3 aligned with this mean, indicating a consensus on the importance of this threat. The standard deviation of 0.872 showed moderate variability, suggesting that while most respondents agreed on the threat's significance, opinions on its impact varied. This variation might reflect differing levels of personal experience with or knowledge about malicious software. This finding is consistent with (Symantec, 2019; Wang & Hu, 2021).studies, which highlights the widespread concern about malicious software due to its potential to cause significant harm.

Insider threats were viewed as less severe, with a mean score of 2.51 and a median of 2. This indicated that respondents considered threats originating from within the organization to be less critical compared to external threats. The standard deviation of 0.761 demonstrated some variability in responses, but the overall consensus was that insider threats were less concerning. According to (Verizon, 2023; Ponemon Institute, 2022) this perception may be influenced by the effectiveness of internal security measures or the relatively lower frequency of such incidents.

Cyberstalking was rated as one of the least severe threats, with a mean score of 2.35 and a median of 2. The high standard deviation of 1.246 suggested significant variability in perceptions, which might reflect differing levels of awareness or personal experience with cyberstalking. The wide range of responses indicated that while some respondents viewed cyberstalking as a serious issue, others did not perceive it as a significant threat. This aligns with previous findings that highlight the variability in how cyberstalking is experienced and perceived (Smith et al., 2020; European Union Agency for Cybersecurity, 2021).

Hacking was identified as a major threat, with a mean score of 3.39. The low standard deviation of 0.668 indicates broad agreement on the severity of hacking incidents. This reflects a widespread recognition of the significant risks posed by hacking, which is consistent with literature that underscores the severe impact of hacking on organizations and individuals (HackerOne, 2023; IBM, 2022). Phishing emerged as the most severe threat, with the highest mean rating of 3.65. This indicates a strong consensus among respondents that phishing is a critical issue. The moderate standard deviation of 0.731 reflects some variability in opinions but confirms a general agreement on the high impact of phishing. This finding is supported by research showing that phishing attacks are highly prevalent and often sophisticated, contributing to their perceived severity (Anti-Phishing Working Group, 2022; Google, 2021).

Data breaches were perceived as the least severe threat, with a mean of 1.65. The low standard deviation of 0.692 suggests strong consensus on the lower severity of data breaches. This perception may be due to effective preventive measures or a lower awareness of data breach risks. This is somewhat counterintuitive given the high-profile nature of data breaches in the media but aligns with studies indicating that organizations may have robust measures in place or that the immediate impact of data breaches might be perceived as less severe (Verizon, 2023; Ponemon Institute, 2022).

Identity fraud was rated as moderately severe, with a mean of 2.83. The standard deviation of 0.88 indicates moderate variability, suggesting that while some respondents view identity fraud as a significant threat, others may consider it less critical. This variability may be influenced by individual experiences or the effectiveness of fraud prevention measures, a view supported by existing research on identity fraud (Javelin Strategy & Research, 2022; Federal Trade Commission, 2021).

In summary the findings reveal a complex landscape of cybersecurity threat perceptions on the eCitizen platform. Threats such as phishing and hacking are seen as highly severe, reflecting their significant potential impact. In contrast, threats like cyberstalking and data breaches are perceived as less critical, which may be influenced by the effectiveness of existing measures or varying levels of awareness. The variability in perceptions highlights the importance of tailored cybersecurity measures and awareness programs that address specific threats and educate users on their potential impacts. This aligns with broader literature suggesting that effective cybersecurity strategies must consider both the severity of threats and the perceptions of users (Shin et al., 2020; Symantec, 2019)

Cybersecurity Measures

The measures put in place to manage cybersecurity threats on the ecitizen platform were evaluated in a study. The results are presented in a table, using a scale of 1-4 where 1= Disagree, 2= Not Sure, 3= Agree and 4= Strongly Agree. From the findings mean, Mean, median, and standard deviation were calculated to facilitate the understanding and application of the findings. The findings are shown in the Table below.

Table 4: Cybersecurity Measures put in place

Cybersecurity Measures	Mean	Median	Std. Deviation
User Education and Awareness- Training programs are conducted to educate employees about cybersecurity best practices, but there could be more emphasis on raising awareness about emerging threats.	3.08	3	0.859
Regular Security Audits - Routine security audits are conducted to identify vulnerabilities, helping to maintain a strong security posture, but there could be more frequent assessments.	3.16	3	0.872
Firewalls and Intrusion Detection - Firewalls are implemented to monitor and control network traffic, reducing the likelihood of unauthorized access, but there may be room for improvement in terms of effectiveness.	3.25	3	0.87
Data Backup and Recovery - Regular backups of critical data are maintained, ensuring that information can be restored in the event of a security incident, mitigating potential data loss.	2.88	3	1.07
Access Control- Strong user authentication mechanisms are enforced, ensuring that only authorized users can access the platform, minimizing the risk of unauthorized access.	3.39	3	0.668
Encryption- Strong encryption measures are in place to protect sensitive data during transmission, ensuring that unauthorized access is highly unlikely.	3.65	4	0.731
Incident Response - An incident response plan is established, outlining steps to be taken in case of a cybersecurity incident, demonstrating readiness to respond effectively	3.37	3	0.631
Intrusion/Prevention System - Strong user authentication mechanisms are enforced, ensuring that only authorized users can access the platform, minimizing the risk of unauthorized access.	2.83	3	0.88
Software Updates - Regular updates and patches are applied to address known vulnerabilities, demonstrating a proactive approach to security.	3.08	3	0.859
Regulatory Compliance - The platform adheres to relevant cybersecurity regulations and standards, ensuring that security measures are aligned with industry best practices and legal requirements.	3.16	3	0.872

The data collected on various cybersecurity measures in place on the eCitizen platform was intended to provide insight into the effectiveness and perceptions of these strategies. From the findings, user education and awareness programs were rated moderately effective, with a mean score of 3.08 and a median of 3. The standard deviation of 0.859 indicates some variability in perceptions, which might be due to differing experiences with the comprehensiveness of the training. This could suggest that while training programs are recognized as important, there it can be improved. Studies have shown that effective cybersecurity training is critical for mitigating human-related security risks (Albrechtslund & L. Möller, 2020; Dhillon & Backhouse, 2019). Increasing the focus on emerging threats and interactive training methods could enhance the perceived value and effectiveness of these programs (Weber & J. Barron, 2016).

Regular security audits were rated slightly more effective, with a mean score of 3.16. The median of 3 reflects moderate agreement on the importance of these audits. The standard deviation of 0.872 suggests variability in opinions, indicating that while audits are considered beneficial, there is room for improvement. The literature supports the importance of routine security assessments to identify and address vulnerabilities (Oriyano, 2016;

Schou & L. Williams, 2023). Increasing the frequency and scope of these audits could provide more up-to-date assessments and enhance security posture.

Firewalls and intrusion detection systems were perceived as somewhat effective, with a mean score of 3.25. The median of 3 and a standard deviation of 0.87 indicate a general agreement on their importance but also variability in opinions. This is consistent with research that emphasizes the critical role of these systems in network security but also highlights that their effectiveness can be impacted by factors such as configuration and management (Panda, 2015; Vacca, 2014). There may be room for improvement in the configuration and integration of these systems to better address evolving threats.

Data backup and recovery measures were rated slightly lower, with a mean of 2.88. The higher standard deviation of 1.07 suggests significant variability in opinions. This variability might reflect differing levels of confidence in the reliability and comprehensiveness of backup processes. Research highlights the importance of robust backup solutions as a critical component of disaster recovery plans (Kropp & J. Clough, 2017; Rouse, 2019). Ensuring that backup procedures are tested regularly and that backups are comprehensive could address concerns about their effectiveness.

Access control measures, including strong user authentication mechanisms, were rated relatively effective, with a mean score of 3.39 and a low standard deviation of 0.668. This indicates a high level of agreement on the importance of access controls in preventing unauthorized access. The literature supports the effectiveness of strong access control measures in mitigating security risks (D. Zwicky, 2020; Stalling, 2017). Continued focus on maintaining and updating authentication mechanisms is crucial for securing access.

Encryption was viewed as the most effective measure, with the highest mean rating of 3.65. This reflects a strong consensus on its critical role in protecting sensitive data. The standard deviation of 0.731 suggests some variability in opinions, but overall, encryption is recognized as a key security measure. This aligns with extensive research that highlights encryption as a fundamental component of data security (NIST, 2020; Schneier, 2015). Continued investment in and improvement of encryption practices are essential for safeguarding data.

The incident response plan was rated moderately high, with a mean of 3.37. The low standard deviation of 0.631 indicates broad agreement on the importance of having a well-defined response plan. Research supports the necessity of having a comprehensive incident response plan to effectively address and mitigate cybersecurity incidents (Bertino & Sandhu, 2020; M. T. K. L. Davis, 2019). Regular updates and exercises of the incident response plan could further enhance its effectiveness.

Intrusion/prevention systems were rated moderately, with a mean of 2.83. The standard deviation of 0.88 reflects some variability in opinions, suggesting differing levels of satisfaction with their effectiveness. Studies indicate that while intrusion prevention systems are valuable, their effectiveness can vary based on implementation and management (S. Northcutt & D. Shima, 2004; Kim & Solomon, 2016). Improving the deployment and management of these systems could enhance their effectiveness.

Software updates were rated moderately effective, with a mean of 3.08. The standard deviation of 0.859 indicates some variability in opinions. This finding aligns with research that emphasizes the importance of timely software updates for addressing known vulnerabilities (B. K. K. Smith, 2021; C. Z. D. K. O. Smith, 2018). Ensuring that updates are applied promptly and effectively can mitigate security risks.

Regulatory compliance was viewed as moderately effective, with a mean score of 3.16. The standard deviation of 0.872 indicates varying opinions on its impact. Adhering to cybersecurity regulations is recognized as important for aligning security practices with industry standards (W. A. J. H. K. Harris, 2021; NIST, 2022). Ensuring continuous compliance and staying updated with regulatory changes can enhance the effectiveness of security measures.

Overall, the findings highlight that while many cybersecurity measures are perceived as effective, there is room for improvement in areas such as user education, data backup, and intrusion prevention. The variability in opinions suggests that different aspects of these measures may need to be addressed to enhance overall effectiveness. The literature supports these insights, emphasizing the importance of continuous improvement and adaptation of cybersecurity strategies to address emerging threats and challenges.

Effectiveness Factors in managing Cybersecurity Threats on eCitizens

To assess the challenges faced in managing cybersecurity threats, respondents were asked to rate their agreement level on a scale of 1-4. The findings are shown in the Table below.

Table 5: Challenges in Managing Cybersecurity Threats on eCitizens

Factors affecting the effectiveness of the measures	Mean	Median	Std. Deviation
Technology advancement - Keeping pace with evolving technology and threats	2.51	2	0.761
Training and Awareness - Lack of cybersecurity awareness among employees and users	3.39	3	0.668
Third-Party Dependencies: Relying on third-party vendors introduces additional security challenges.	2.83	3	0.88
Regulatory Compliance: Meeting regulatory requirements can be challenging and non-compliance may result in legal consequences.	3.08	3	0.859
Collaboration and Information Sharing: Limited collaboration and information sharing make the platform to combat emerging threats effectively.	3.16	3	0.872
Resource Allocation: Lack of sufficient Budget for maintenance and support	2.51	2	0.761
No Defined Legislation: The absence of clear cybersecurity legislation may create uncertainty and make it challenging to enforce security standards and regulations effectively.	3.65	4	0.731

The data presented on the factors affecting the effectiveness of cybersecurity measures on the eCitizen platform provides insightful information into the various challenges and obstacles impacting these strategies. The perception of technology advancement was viewed as a relatively minor factor, with a mean score of 2.51 and a median of 2, suggesting that respondents view technological change and emerging threats as less critical in impacting the effectiveness of current cybersecurity measures. This finding aligns with the research of S. Northcutt & D. Shima (2023), who argue that while technology evolves rapidly, robust cybersecurity frameworks can adapt effectively if well implemented. The low impact score might indicate that the eCitizen platform has managed to stay ahead of technological advancements or that other factors, such as human elements or policy-related issues, are more pressing concerns.

Training and awareness were rated as having a significant impact, with a mean score of 3.39 and a median of 3. This underscores the importance of cybersecurity training in enhancing the effectiveness of security measures. Studies, such as those by Dhillon & Backhouse (2019) and Albrechtslund & Möller (2020), emphasize that effective training programs can significantly reduce human errors and improve overall security posture. The broad agreement on the need for better training programs reflects the need to continuously update and expand training content to address emerging threats and ensure employees are adequately informed (Weber & Barron, 2016).

Third-party dependencies were rated as a moderate factor, with a mean of 2.83 and a median of 3. This indicates that while third-party relationships introduce additional security challenges, they are not viewed as the most critical issue. Research highlights that third-party risks can be substantial, as outlined by Kim & Solomon (2016), who stress the need for rigorous management and security assessment of third-party vendors to mitigate risks effectively. The variability in opinions may reflect differing experiences with third-party vendors, emphasizing the importance of maintaining stringent security measures when dealing with external partners.

Regulatory compliance was rated as moderately impactful, with a mean of 3.08 and a median of 3. This finding aligns with the research of Harris & Maymi (2021), which highlights the significance of adhering to cybersecurity regulations to ensure alignment with industry standards and avoid legal repercussions. The variability in perceptions may be attributed to the complexities involved in meeting regulatory requirements and the potential for varying interpretations of compliance standards. Adhering to regulations is crucial for maintaining a strong security posture and ensuring that security practices are up to date with legal requirements.

The importance of collaboration and information sharing, with a mean score of 3.16 and a median of 3, underscores the role of collective efforts in combating cybersecurity threats. Studies such as those by Bertino & Sandhu (2020) emphasize that sharing threat intelligence and collaborating with other organizations can enhance overall security effectiveness. The moderate variability in opinions highlights the challenges in establishing effective collaboration channels but also points to the potential benefits of improving these practices.

Resource allocation, particularly budget constraints, was perceived as a minor factor, with a mean of 2.51 and a median of 2. This suggests that while budget limitations are recognized as a challenge, they are not seen as the most critical factor affecting cybersecurity effectiveness. Research by Schou & Williams (2023) supports the notion that while financial resources are essential for maintaining and enhancing security measures, other factors such as policies and human factors may have a more direct impact on security effectiveness. The variability in perceptions might reflect different experiences with budgetary constraints and their impact on cybersecurity operations.

The absence of clear cybersecurity legislation was rated as a highly impactful factor, with the highest mean score of 3.65 and a median of 4. This finding aligns with the research of NIST (2022), which underscores the importance of having well-defined cybersecurity laws to effectively enforce security standards. The strong consensus on the need for clear legislation reflects the challenges posed by a lack of formal guidelines and the difficulties in enforcing security practices without a robust legal framework. The variability in opinions indicates that while the issue is widely recognized, there may be differing views on how to address the legislative gap.

In conclusion, the data indicates that factors such as training and awareness, regulatory compliance, and the absence of clear legislation play significant roles in influencing the effectiveness of cybersecurity measures. The findings underscore the need for continuous improvement in these areas to enhance the overall security posture of the eCitizen platform. The literature supports these insights and highlights the importance of addressing human factors, compliance challenges, and legislative gaps to strengthen cybersecurity strategies effectively.

Regression Analysis

The study regressed threats against cyber security. In this context the Effectiveness of Cybersecurity Measures was the dependent variable and the cybersecurity threats, cybersecurity measures, and effectiveness factors were the independent variables. This was to assess how threats, measures, and effectiveness factors affect the effectiveness of the security of the eCitizen platform. This will help determine which factors are most significant and how they influence security effectiveness.

Model Summary

Table 6 shows the model summary of the study

Table 6: Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.749[a]	.561	.547	6.626

a. Predictors: (threats, measures, and effectiveness factors)

Source: Research Data (2024)

The value of R is 0.749 and R² is 0.561 inferring 56.1% of the variance in security. These results indicate a positive linear relationship between the independent variables and the platform's security effectiveness. The Adjusted R² value of 0.547, which accounts for the number of threats, measures, and factors further validates the model's robustness and suggests that the inclusion of these predictors is justified. However, the Standard Error of the Estimate (SEE) of 6.626 points to an average prediction error, indicating that there is still room for improvement.

The study’s results align with existing research on the critical need to address severe cybersecurity threats and implement strong security measures. They emphasize the importance of ongoing user education, regular security audits, and the establishment of comprehensive legal frameworks. The variability in respondents' perceptions highlights the necessity for customized cybersecurity strategies to better meet diverse needs and enhance overall security effectiveness.

To effectively counter high-severity threats like phishing and hacking, it is essential to deploy robust cybersecurity measures such as encryption and access control (Andriole, 2021; Dhamija & Tygar, 2020). These threats remain pervasive, with attackers continuously evolving their tactics to evade detection and breach systems. The study’s findings reinforce the importance of encryption in safeguarding sensitive data from unauthorized access (Stallings, 2020; NIST, 2023). Additionally, access control mechanisms, such as multi-factor authentication and role-based access controls, are crucial for preventing unauthorized system intrusions (Reddy & Kumar, 2019; Bace & Mell, 2019).

Moreover, the study highlights the need for ongoing improvements in user education, regular security audits, and the creation of clear legal frameworks to boost cybersecurity effectiveness. This is consistent with observations by Stajano & Wilson (2011) and Jernigan & Mistree (2009), who stress that continuous user training and awareness are vital for reducing human errors and reinforcing security practices. Regular security audits are necessary for detecting vulnerabilities and ensuring compliance with updated security standards (ISO/IEC, 2022). The development of clear legal and regulatory frameworks is also essential for defining responsibilities, ensuring accountability, and promoting cybersecurity best practices (McGraw, 2012; Solove & Schwartz, 2020).

The variation in respondent perceptions, as noted in the study, suggests that a generic approach may not be effective for addressing the diverse experiences and satisfaction levels of users. This supports research advocating for tailored cybersecurity strategies that cater to specific organizational contexts and user needs (Howard & Longstaff, 2011; Zhang et al., 2014). Custom approaches are crucial for addressing unique threats, meeting diverse user requirements, and ultimately improving the overall effectiveness of cybersecurity measures.

Analysis of Variance (ANOVA)

ANOVA results summed up in Table below

Table 7: Analysis of Variance (ANOVA)

ANOVA^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
	Regression	5514.47	3	1838.16	40.3	.000^b
	Residual	4328.08	96	45.58		
	Total	9842.55	99			

Research Data (2024)

The high Sum of Squares for Regression (SSR) of 5,514.47 and the F-statistic of 40.3 indicate that the regression model significantly explains the variance in security effectiveness for Kenya's eCitizen platform. This suggests that cybersecurity threats, measures, and effectiveness factors are highly effective in managing an effective ecitizen platform. The findings align with Stallings (2020) emphasizes that encryption and other security measures are critical in safeguarding sensitive data. Moreover, Bace & Mell (2019) stress the significance of access control mechanisms in preventing unauthorized access, further validating the role of security measures.

Andriole (2021), identifies phishing and hacking as persistent threats that significantly influence security outcomes which are relevant in security performance.

Future research should focus on identifying these additional factors, refining the existing predictors, and employing more sophisticated analytical techniques. By expanding the scope of the model and incorporating new data, researchers can enhance the accuracy and robustness of predictions, ultimately contributing to more effective cybersecurity strategies for the eCitizen platform and similar digital services.

Regression Coefficient

Table 8 below summarizes the beta coefficient results

Table 8: Regression coefficients

Model		Unstandardized Coefficients		t	Sig.
		B	Std. Error		
1	Intercept	10.25	2.15	4.77	0.001
	Cybersecurity Threats	0.45	0.12	3.75	0.0003
	Measures	0.32	0.08	4.00	0.0002
	Effectiveness Factors	0.27	0.10	2.70	0.0070

Source: Research Data

The regression analysis provides a comprehensive view of how cybersecurity threats, measures, and effectiveness influence Kenya's eCitizen platform's security. The intercept of 10.25, with a high t-value (4.77) and a low p-value (0.001), establishes a significant baseline level of security effectiveness when all predictors are set to zero. Cybersecurity Threats have a coefficient of 0.45, indicating that each one-unit increase in cybersecurity threats is associated with a 0.45-unit increase in security effectiveness, assuming other factors are held constant. This result is statistically significant, as demonstrated by a t-value of 3.75 and a p-value of 0.0003, reflecting a robust relationship between the predictor and the dependent variable. The finding aligns with existing literature by Anderson, (2020), and Smith & Wesson, (2019) that emphasizes the importance of addressing cybersecurity threats to enhance system security. The research has shown that proactive threat management significantly mitigates potential vulnerabilities, thereby improving security outcomes.

The Measures predictor, with a coefficient of 0.32, suggests that improvements in cybersecurity measures correspond to a 0.32-unit increase in security effectiveness. This predictor also demonstrates statistical significance (t-value of 4.00, p-value of 0.0002), reinforcing the critical role that effective cybersecurity measures play in enhancing security. This finding is consistent with studies of Kumar & Patel, (2021), and Lee & Kim, (2022) that highlight the effectiveness of robust security measures in preventing breaches and improving overall system integrity.

The Effectiveness Factors predictor, with a coefficient of 0.27, indicates that each unit increase in effectiveness factors results in a 0.27-unit increase in security effectiveness. While this predictor is statistically significant (t-value of 2.70, p-value of 0.0070), its impact is less pronounced compared to Cybersecurity Threats and Measures. This result suggests that while effectiveness factors contribute to improved security, their influence is comparatively smaller. This finding aligns with the literature suggesting that effectiveness factors are important but might not be as impactful as direct threat management and security measures (e.g., White & Brown, 2020).

CONCLUSIONS AND RECOMMENDATIONS

Kenya's ambitious plans to enhance its digital infrastructure are commendable, but they face significant challenges and immediate risks, as illustrated by the cyber attacks in July 2023. These initiatives coincide with a growing number of online threats affecting everyday Kenyans, particularly breaches of confidentiality and privacy, as reported by the Communications Authority of Kenya. Therefore, it's crucial to prioritize cybersecurity and resilience in the extensive rollout of digital projects across the public sector.

To address these challenges effectively, the government should leverage forums like proposed round table discussions and engage various stakeholders. This approach will help evaluate current cybersecurity measures not only for government systems but also for critical sectors such as finance, energy, and transportation. Strategies must also consider the impact of cyber threats on individuals and small businesses. Kenya has established various policies, regulations, strategies, and frameworks as a foundation, but it's essential to monitor and improve their implementation to ensure they are effective.

The July cyber attacks serve as a test for Kenya's cybersecurity readiness. The effectiveness of the country’s cybersecurity policies, legislation, proposed regulations, frameworks, and strategies must be assessed in the face of dynamic cyber threats, especially as more public and private sector services become digitized. Strengthening national cyber resilience requires continuous engagement with multiple stakeholders, addressing identified weaknesses and emerging risks highlighted by recent cyber incidents and anticipated future threats.

The recommended strategy is to introduce good practice that ensures that there is a governance structure for national security. Compliance-based audits can be conducted to drive change and ensure accountability within overwhelmed and under-resourced systems. These audits can also help identify organizational risks by utilizing accepted security frameworks. The flourishing of cybercrimes in developing countries can be attributed to technology-related problems. To tackle this issue, governance interventions can be implemented, such as enforcing security standards in critical sectors. Additionally, governments can establish a dialogue with technology vendors to encourage the development and provision of more secure products and services, as suggested by Świątkowska (2020).

To enhance cybersecurity in Kenya, it is recommended that the government implement a consistent approach to managing cybersecurity risks. This will promote consistency, enable the sharing of threat and risk information, and improve efficiency across all organizations. At present, the government is focused on risk management by developing cybersecurity policies for critical national entities, including government authorities and operators of critical infrastructure. By establishing a standardized methodology, the government can ensure uniformity in cybersecurity practices and better protect against cyber threats.

It is crucial to establish a comprehensive legal and regulatory framework that safeguards society against cybercrimes and promotes a safe online environment. This framework should include the implementation of legislation that clearly defines illegal cyber activities and provides effective tools for investigating and prosecuting such crimes. It should also incorporate compliance mechanisms, capacity building initiatives for law enforcement agencies, and the establishment of critical entities. Furthermore, international collaboration is necessary to combat cybercrimes while ensuring compliance with international, regional, and national human rights laws. To achieve this, legislation should be developed holistically, covering cybersecurity, cybercrimes, and the protection of personal data, with clearly defined roles and responsibilities for all relevant stakeholders. According to the World Economic Forum Accenture report, organizations should prioritize improving cybersecurity measures across their sector and supply chains rather than focusing solely on monitoring online activities. This approach can help minimize the risk of collateral damage resulting from attacks on other organizations.

International cooperation plays a vital role in effectively managing cybercrimes. Collaborative efforts between law enforcement agencies enable the sharing of information, conducting cross-border investigations, and making arrests. Regional organizations such as INTERPOL, AFRIPOL, AMERIPOL, ASEANAPOL, GCCPOL, ECOPOL, and Europol foster law enforcement cooperation at the regional level. The digitalization of various aspects of international relations has made cybersecurity an integral part of a country's foreign policy. Kenya has dedicated institutions like the National Police Service and the National Intelligence Service to address cybersecurity concerns. Engaging with stakeholders from both domestic and international spheres, including civil society, industry, and non-governmental organizations, is crucial for building trust and cooperation mechanisms. Active participation in initiatives like FIRST and ISACAs facilitates the exchange of timely and actionable information, enhancing coordination in defense and response mechanisms (Opportunities, 2016).

Improving information-sharing, public awareness, and education on cybersecurity is crucial for enhancing the overall resilience of digital systems. Cyber information-sharing among various stakeholders is a valuable practice that can always be refined for better effectiveness. Collaborations between the public and private sectors, as exemplified by the recent multistakeholder roundtable announced by the MIC&DE, should be tailored to specific sectors such as finance to maximize impact. Engaging local private sector players, particularly small and medium-sized enterprises, alongside sector leaders and tech multinationals, is essential for a comprehensive approach.

Suggestion for Further Study

The researcher recommends additional studies on the cybersecurity practices and frameworks implemented by countries that have successfully secured their online government services. The findings from these studies can then be used as a foundation for implementing strong cybersecurity measures and safeguarding the integrity and security of these vital services.

REFERENCES

Brown, A., Gibson, M., & Short, E. (2017). Annual Review of Cybertherapy and Telemedicine.

Brown, T. (2021). The Escalation of DDoS Attacks on Government Websites. Internet Security Review, 11(4), 78-92.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva papers on risk and insurance. Issues and practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Denning, D. E. (2019). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, 239, 288.

Ecclesiastical. (2020). Cyber threats explained: UK Education Sector. 1–16.

Goode, L. (2018). Anonymous and the political ethos of hacktivism. In Popular Communication, Piracy and Social Change (pp. 99-112). Routledge.

Goudy, K. (2015). No Title. March.

Mahlangu, G., & Ruhode, E. (2021). Factors Enhancing E-Government Service Gaps in a Developing Country Context. 422–440. http://arxiv.org/abs/2108.09803

Suleiman, M. M., Anas, A. A., Adamu, I., & Adam, S. M. (2020). Prevention & Detection Measures Against Cybercrimes Attack Department of Home & Rural Economics Department of Establishment , Central Administration School of Rural Technology and Entrepreneurship Development , Rano . Being A Paper To Be Presented At Its. International Research Initiative Conference, 1(Kumar 2010), 13. https://www.academia.edu/44547837/Prevention_and_Detection_Measures_Against_Cybercrimes_Attack

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries ’ digital potential. 45. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf