06

Cyber Espionage Vulnerabilities in Kenya's E-government Ecosystem: A Case Study of a Public Institution

George K. Karoki, Irene Mukiri Mwingirwa, and Sam Kamau

Abstract

The rapid advancement of information technology in Kenya has ushered in the digital era, revolutionising the government's service delivery through e-Government. However, the transformation has inadvertently exposed government systems, databases, and infrastructures to the threat of cyber espionage, leading to unauthorised access to sensitive data. The aim of the study is to assess cyber espionage vulnerabilities within Kenya's e-Government ecosystem with a specific case study of a public institution (PI)*. By addressing this critical issue, the article seeks to ensure the integrity, confidentiality, and availability of sensitive information, protect national security interests, and sustain the progression of e-Government initiatives. The study was grounded in game theory. To ensure comprehensive data collection and bolster the validity and reliability of the study, a mixed-methods approach was employed, encompassing both quantitative and qualitative data. The study focused on system end-users, ICT officers, system auditors, and ICT manager to offer an encompassing perspective as conveyed by the participants. The study established that though the government deploys information technology to boost service delivery, such deployment has not been matched by measures to address automation weaknesses that could provide opportunities for cyber espionage attacks. The researcher recommends that PI should update and implement its information security policy to encompass current and emerging cybersecurity issues, enhance employee training and awareness through robust training programs, and use technology such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to enhance their detection and prevention capabilities.

Keywords: Cyber espionage, threats, e-Government, ecosystem, public institution

*PI is a pseudonym for a public institution in Kenya which utilises e-government services.

Introduction

Governments and organisations worldwide have continually invested significantly in Information Communication Technology (ICT) and telecommunications infrastructure (Alderete, 2018). This continuous digital revolution has yielded unprecedented global affluence and efficiency, positively impacting the adoption of electronic government (e-Government) initiatives across government ministries, departments, and organisations (Nyonje et al., 2018). In Kenya, a government agency which for purposes of this study will be referred to as Public Institution (PI) has made significant efforts towards digitising its services to improve efficiency and transparency through the e-Government systems. However, the move has opened up new avenues for cyber espionage attacks as an increasing amount of sensitive information is being digitalised and stored online, which could put the PI and citizens at risk.

E-Government entails providing a wide range of government services and disseminating information to its citizens through the utilisation of Information and Communication Technology (ICT) applications (Malodia et al., 2021). Adopting e-Government improves efficacy, efficiency, and service delivery of government and public administration procedures and services. Cyber espionage, on the other hand, is the use of computer networks and digital communication activities to gain unauthorised access to sensitive and confidential data and information, usually in a government's or other organisation's possession (Herrmann, 2019). Given their handling of confidential and personal identifiable information, e-Government systems are particularly attractive targets for cyber espionage attacks. The attacks can be perpetrated by state-sponsored groups, criminal organisations, hacktivists, or individual hackers. This fuels apprehensions that no government or institution remains immune within the concealed realms of cyberspace.

Cyber espionage has emerged as a sinister and growing concern across the global public sector, employing state-of-the-art techniques to clandestinely, efficiently, and continuously gather crucial information (Rudner, 2013). Moreover, the technology and information systems utilised within the public sector are experiencing rapid expansion, along with the availability of resources and services, thus amplifying the vulnerability to cyber espionage and data breaches (Cremer et al., 2022).

Kenya's journey toward e-Government began in 2004 after the government approved an e-Government policy. In 2006, the Ministry of Information and Communications (MoICT) further endorsed the National ICT policy, guiding human resource development, infrastructure expansion, stakeholder engagement, and regulatory framework establishment (Mungai, 2017). Subsequently, the government initiated several e-Government projects to enhance the efficiency, transparency, and democratic processes of public administration (Wamoto, 2015). Notable initiatives include the G-pay system, streamlined passport application and processing, the e-Registry for business registration, i-Tax for Kenya Revenue Authority (KRA) services, and eCitizen. PI has embraced digital transformation to improve service access and efficiency. This transition has streamlined operations and created a comprehensive database that is valuable for faster and expanded delivery of services. As well, the use of digital information makes it easy for the Organisation to link with other government departments.

Government institutions have of late increasingly become focal points for cyber espionage attacks. A 2020 report by Verizon's data breach investigation professionals revealed that between 2014 and 2020, the public sector worldwide experienced 2,152 data breaches, with cyber espionage accounting for nearly 31% of these incidents (Verizon, 2020). Such threats potentially breach the security of highly sensitive data. Exploiting such information poses substantial risks, including, but not limited to, identity theft, the perpetration of phishing scams, fraudulent activities, financial theft, unwarranted harassment, and the stalking of individuals.

In February 2023, Medusa hackers reportedly used the identity card and passport of one of Kenya Airport Authority's (KAA) engineers to gain access to the Authority's network, leading to the leakage of 514 GB of data, including site surveys, procurement, plans invoices, physical plans, and receipts on the internet (Wanjala, 2023). Further, Kenya's eCitizen system, a digital platform enabling citizens and clients to access government services online, was cyber attacked in July 2023 by hackers operating under the name "Anonymous Sudan" (Carletti, 2023). The consequences of these breaches extend beyond compromising the integrity of sensitive information's, availability, and confidentiality, potentially endangering national security and undermining public trust.

This study examines cyber espionage threat vulnerabilities within the e-Government ecosystem in Kenya's PI. It set out to answer the question: What are the prevailing cyber espionage vulnerabilities within the PI e-Government ecosystem? In response, this article examines the vulnerabilities in the PI e-Government ecosystem by shedding light on the specific vulnerabilities and providing recommendations to bolster the cyber security posture.

The quest for e-Government growth and adoption by government institutions has impacted institutions' preparedness for threats and exposed vulnerabilities that can be exploited for cyber espionage. Even though each industry's cyber espionage threat vulnerabilities are unique, the public sector consistently ranks at the top of the sectors subjected to numerous cyber attacks (KNBS Economic Survey, 2022).

The study provides suggestions and proposes a framework to help ministries and departments safeguard their systems and protect public and government data. It also forms a basis for policy formulation by providing current and emerging cyber espionage vulnerabilities in Kenya's e-Government ecosystem that are susceptible to cyber criminals.

Statement of the problem

Kenya faces cyber espionage activities carried out by non-state actors, which include criminal organisations and hacktivist groups, in addition to state-sponsored threats. These entities frequently target government systems, research organisations, businesses, or individuals with sensitive information access (Onyando, 2023). These cyber actors often employ advanced methods, such as malware injections, spear-phishing, and social engineering tactics, to gain unauthorised access to target systems and Information Technology (IT) infrastructures. Their aim may include stealing sensitive information, disrupting systems, and causing reputational damage. Notably, these tactics continually evolve in response to the changing threat landscape. Yet the e-Government ecosystem exhibits vulnerabilities that could expose Kenya to cyber insecurity. Therefore, it is imperative to assess the current and emerging cyber espionage vulnerabilities in Kenya's e-Government ecosystem that are susceptible to cyber criminals and offer suggestions for safeguarding public and government data.

Literature review and theoretical framework

Cyber espionage threat

Espionage has long fascinated states, organisations, and the public, particularly during the Cold War when the United States and the USSR escalated espionage activities. However, the landscape of espionage, or spying, has undergone significant transformation in recent years. Today, states and organisations grapple with the complexities of an ever more interconnected cyber world, where technology often advances at a pace that outstrips the ability of policymakers to adapt (Dilanian, 2021). This shift and the simultaneous growth of Information Systems and Technology (IS&T) and globalisation has given rise to cyber espionage orchestrated by foreign governments, criminal organisations, state-sponsored organisations, and individuals.

Cyber espionage has a relatively recent origin but has undergone swift evolution in recent decades. Its inaugural documented occurrence dates back to the 1980s when the Soviet Union clandestinely employed computer viruses to gather intelligence from Western nations. Subsequently, cyber espionage expanded in tandem with technological progress and the widespread proliferation of the internet (Akram & Malik, 2023). It has instilled a heightened sense of apprehension in nations worldwide due to the inherent ambiguity surrounding the intentions of adversaries, the challenge of attribution, and the absence of a robust legal framework for prosecuting suspected cyber criminals (Pun, 2017).

In the intricate and ever-evolving landscape of contemporary security, global cyber espionage threats exhibit a dual nature, effortlessly crossing national boundaries and outpacing the traditional security measures and capacities that states have traditionally depended on to safeguard their interests and enhance their security stance (Li & Liu, 2021). For instance, in 2015, Chinese hackers executed a cyber-espionage operation targeting the United States Office of Personnel Management (OPM). This exposed personal data from over 22 million individuals (Nakashima, 2015).

The emergence of highly sophisticated targeted information thieves has significantly impacted the cyber espionage landscape, recently. In this altered landscape, nations find themselves confronted by a wide array of adversaries, yielding multiple potential entry points, as opposed to the past when they primarily contended with one or a few nation-state adversaries (Rubenstein, 2014). A notable example of this threat occurred in September 2022 when Optus, Australia's second-largest telecommunications provider, fell victim to a cyber espionage attack. This breach led to the unauthorised access and theft of sensitive information belonging to approximately ten million citizens (Shepherd, 2022). In March 2022, the United Kingdom (UK) and the United States also exposed Russia's Federal Security Service (FSB) for its historical malicious cyber espionage activities. Both countries asserted that the FSB had employed advanced spear-phishing techniques to target crucial national infrastructure sectors, including the US aviation and UK energy sectors (Gov.uk, 2022).

Africa has experienced a remarkable surge in adopting information and communication technology (ICT) and internet connectivity. This digital transformation has resulted in an expanding user base and the gradual integration of digital technologies in government agencies. However, this widespread digitalisation has also opened numerous new entry points for malicious cyber actors seeking to access governments' and organisations' networks (Velluet, 2023).

Cyber espionage poses a growing and substantial threat to Africa, as the continent rapidly advances its technological infrastructure. Unfortunately, many African nations lack the resources and expertise to mount effective defences against such espionage. This makes them vulnerable targets (Samme-Nlar, 2023). State-sponsored hackers and criminal groups frequently direct their efforts towards African countries, seeking sensitive information like trade secrets, national security data, and personal information of government officials and citizens. This primary threat typically originates from state actors outside the continent, as demonstrated by China's unauthorised access to crucial data within the servers and information systems of the African Union (AU) headquarters, which they compromised in 2018 (Reuters, 2018). Furthermore, cyber espionage involved the Pegasus malware infiltrating computer systems in 11 African countries, enabling data collection and domestic surveillance activities (Maschmeyer et al., 2021).

African nations generally demonstrate limited cyber maturity and possess constrained offensive and defensive cyber capabilities. They rely heavily on foreign entities for critical information infrastructure and data management through cloud technologies. This reliance significantly limits their control over electronic information generated by their citizens and renders the technological infrastructure in many countries across the continent vulnerable to potential cyber espionage compromise (Waag-Cowling, 2021; (Africa Defense Forum, 2022). For instance, a Chinese company, Huawei, manufactures approximately 70% of 4G base stations in Africa and is also poised to lead the 5G market. This situation raises concerns as it implies potential external control over critical information infrastructure. This external influence could lead to compromise, sabotage, or the introduction of covert attacks and vulnerabilities into the supply chain (Welle, 2022).

In Kenya, cyber espionage is an escalating threat driven by widespread internet access amplified by high-speed fiber optic connections and the increasing adoption of information systems within government agencies and institutions. As government agencies and organisations increasingly rely on information systems, there is a heightened risk of malicious actors stealing sensitive information through hacking and other cyber attacks. Cybersecurity reports highlight a significant increase in cyber espionage attacks within Kenya, primarily focused on unauthorised data acquisition (Sang, 2022).

Cyber attacks on Kenya's e-Government systems, such as the July 2023 incident targeting the eCitizen portal, can have extensive repercussions, affecting countless citizens and severely disrupting essential services. Notably, services such as passport and visa applications, National Transport and Safety Authority (NTSA), Directorate of Criminal Investigation (DCI), as well as mobile-money banking experienced significant disruptions, leading to widespread inconveniences (Vandyck, 2023). In April 2016, a cyber espionage group posing as "Operation Africa" executed an intrusion into Kenya's Ministry of Foreign Affairs. During this breach, they conducted phishing attacks and acquired various documents, including diplomatic correspondence between Kenyan foreign ministry representatives and other diplomatic missions, international trade partners, and global businesses (Agutu, 2016).

Cyber espionage vulnerabilities

Attackers exploit the vulnerabilities, often combining one or more, to break privilege boundaries (perform illegal operations) within a computer system. A vulnerability is a defect in a system that an attacker can exploit to conduct a successful attack (Luiijf, 2012). They arise due to defects, features, or user errors (Thompson et al., 2002). A system weakness or vulnerability must be connected to by an attacker using at least one appropriate instrument or technique. Through security flaws, attackers access information systems and networks and potentially access important and sensitive data (Xu et al., 2019). Given that a chain is only as strong as its weakest link, the security posture of government information systems is as robust as its weak points.

Theoretical framework

In the context of the e-Government ecosystem, game theory and the Moving Target Defence (MTD) approach play crucial roles in understanding cyber espionage threat vulnerabilities and developing effective defence strategies. Game theory, endorsed by renowned figures such as John Nash, Thomas Schelling, and John von Neumann, revolves around key tenets: players, actions, payoffs, and strategies. Players, whether individuals or entities, pursue distinct goals, aiming to maximise their utility through strategic actions. Each action, taken by a player at every turn, is influenced by their awareness of others' actions. Ultimately, players receive payoffs at the end of the game, reflecting the utility gained from outcomes, positive or negative. Strategies, tailored for each player, are crafted based on opponents' past and anticipated actions, targeting victory in the game (Douha et al., 2023). By modelling these interactions, game theory helps identify optimal strategies for reducing the likelihood of cyber espionage attacks and illuminating potential vulnerabilities (Pătraşcu & Simion, 2013).

Game theory, however, has limitations, such as scarcity of information about attackers' strategies and the assumption of rational attacker behaviour (Patil et al., 2018). The Moving Target Defence (MTD) approach, championed by proponents such as Salman Base and Yan Chen, is employed to address these limitations. The MTD approach is built on four core principles. First, it continuously changes system characteristics to thwart attackers' attempts to identify and exploit vulnerabilities. Second, MTD uses decoys that mimic genuine assets, diverting attackers and providing defenders with time to detect and respond to threats. Third, it actively disrupts attackers by blocking IP addresses, slowing network connections, or impeding their access. Lastly, MTD dynamically adjusts system components, like reconfiguring firewalls and access controls, in real-time to counteract attackers effectively (Lei et al., 2018). By continuously changing the attack surface and making it difficult for attackers to identify and exploit vulnerabilities, MTD significantly enhances cybersecurity and makes systems counteract attackers effectively (Lei et al., 2018). By continuously changing the attack surface and making it difficult for attackers to identify and exploit vulnerabilities, MTD significantly enhances cybersecurity and makes systems more resistant to cyber espionage attacks.

In the context of the e-Government ecosystem, game theory and the Moving Target Defence (MTD) approach are instrumental in comprehending vulnerabilities and bolstering cybersecurity. Game theory analyses the dynamics between cyber defenders and attackers, considering factors like vulnerability assessment and attackers' behaviour.

Methodology

The study employed a mixed-methods approach, utilising questionnaires and interviews to collect quantitative and qualitative data. The research was conducted in PI offices in Nairobi. To protect sensitive information and maintain ethical standards, the organisation central to this study has been anonymised. The study employed stratified random sampling for quantitative respondents and purposive sampling for interviews. Questionnaires were distributed to 48 e-Government systems end-users, and interviews were conducted with ICT officers, a System Auditor, and an ICT manager. Pre-testing was conducted to improve the instruments, and data analysis involved statistical techniques for quantitative data and narrative construction for qualitative data. Necessary permits and consents were obtained from PI management and participants, ensuring anonymity, confidentiality, and voluntary participation.

Findings and discussion

The study reveals that the government has made efforts to address vulnerabilities that cyber actors could potentially exploit in carrying out illicit activities, including promoting robust passwords. However, the findings show several existing vulnerabilities, as highlighted below.

Technological vulnerabilities

These are vulnerabilities that exist within Kenya's e-Government systems, including potential weaknesses in network infrastructure and software applications. The findings of the study shed light on several specific vulnerabilities that merited attention. One noteworthy issue is the absence of up-to-date computer antivirus software, which exposes the e-Government systems to a heightened risk of malware and other cyber threats. Misconfigured firewalls also present as a weak point in the system framework, as they can inadvertently allow unauthorised access and data breaches. Software misconfigurations and the applying system patches designed to rectify security vulnerabilities or system bugs further compounds the vulnerabilities, creating security gaps that malicious actors could potentially exploit. These vulnerabilities pose significant risks to the security and stability of Kenya's e-Government systems, potentially exposing them to cyber espionage threats and unauthorised access.

The findings among system users surveyed revealed that an overwhelming majority, comprising 39 individuals (86.7%), had antivirus software installed on their computers, indicating a positive level of compliance with basic cybersecurity measures. In contrast, a small proportion of users, accounting for 3 respondents (6.7%), had no antivirus protection, while 3 respondents (6.7%) did not know whether they had antivirus installed on their computers, indicating a potential lack of awareness or knowledge about the security measures in place on their devices. This suggests that the organisation's efforts to raise awareness and promote antivirus use among its employees' computers have been relatively successful. Although the majority had antivirus software, the presence of those who did not have it and those who were unsure if they had it acted as a potential security gap.

Some respondents noted that most of the users in the organisation use expired antivirus software that requires renewal, meaning that computers are not getting critical updates and protection against the most recent malware and cyber threats. The study findings indicated that a substantial portion of system end-users, 26 individuals (57.8%), update their antivirus software as needed, demonstrating awareness and proactive cybersecurity behaviour. Conversely, a smaller group of users, 6 (13.3%), admitted never having updated their antivirus protection. This is troubling as outdated software is less effective at protecting against new and evolving threats, leaving computers and systems vulnerable to cyber espionage attacks. Further, 5 users (11.1%) adhere to a monthly update schedule; 2 users (4.4%) opt for quarterly updates; and 6 (13.3%) reported an annual update frequency for their antivirus software. These results show a lack of standardised cyber security practice within the organisation.

Antivirus software is crucial for detecting and mitigating malware, thus reducing the risk of successful espionage attacks. It detects, blocks, quarantines, or deletes malware, and antivirus vendors regularly update their software to include new threat signatures as cyber espionage techniques evolve. Cybersecurity experts, such as Janczewski and Colarik (2007), Pérez-Sánchez and Palacios (2022), and Shah and Comissiong (2021) emphasise the importance of antivirus updates in protecting systems from new viruses. The insights of the Cybersecurity Infrastructure and Security Agency (CISA) align with the findings of this study, highlighting the necessity of maintaining up-to-date antivirus signatures based on known characteristics of malware (CISA, 2019).

In addition to antivirus software, properly configured firewalls act as critical defences against cyber threats like espionage by safeguarding system networks

In addition to antivirus software, properly configured firewalls act as critical defences against cyber threats like espionage by safeguarding system networks from unauthorised external access. Rouse (2022) and Anwar et al. (2021) confirm that firewalls serve as traffic controllers, validating and managing client network access, and play a pivotal role in mitigating cyber threats. Misconfigurations in software and systems, especially in network devices, servers, and applications, create security flaws that cyber espionage actors exploit. This allows them to conduct espionage activities. Failing to apply patches and updates to software and systems exposes them to known vulnerabilities, which cyber actors can exploit for unauthorised access and cyber espionage, as noted by Analytica (2021) and Bello et al. (2022).

Organisational vulnerabilities

Organisational vulnerabilities within the e-Government ecosystem pertain to governance, policies, and internal practices. The study underscored certain deficiencies, particularly in access control mechanisms within PI. This suggests that sensitive data remains susceptible to unauthorised access, alteration, or deletion. This vulnerability raises significant concerns, especially in light of the substantial amount of personally identifiable information stored by the government. Moreover, the absence of robust regulations and enforcement mechanisms compounds existing vulnerabilities in the e-Government environment. The failure by the government to impose penalties on cybercriminals fosters a perception of a permissive operating environment conducive to illicit cyber activities. Furthermore, the presence of untrustworthy software vendors who retain their super user accounts even after relinquishing control of the system further exacerbates vulnerabilities in the ecosystem.

An analysis of responses from the interviews revealed that systems enable cyber actors to infiltrate, monitor, and extract sensitive information from a targeted system by providing advanced capabilities and tools. Misconfiguration of the systems, lack of patching, and system vendors were found to be the three main vulnerabilities in the organisation that would make the systems susceptible to cyber espionage.

Regarding system vendors, respondent R-SA explained that some vendors continue to have their systems super user accounts even after handing over the system to the recipient organisation and ministry. According to the respondent, vendors should install and train the officers handling the system and hand over the complete system and its source code to the PI. Further, their accounts should be disabled to ensure they cannot access the system after handing over. The respondent narrated:

> *Some vendors who developed or sold some of the systems used at the organisation still have access, and some may be briefcase solution vendors representing other institutions or countries of interest.* (R-SA)

It was a common view among respondents that some outsourced systems already have a backdoor that cyber actors may use to exfiltrate data. The respondents stated there was a need to thoroughly vet the system vendors and source code to ensure no malicious code is incorporated. The respondents retaliated that software vendors should transfer skills, source code, and train Information Technology (IT) managers.

The absence or delay in applying system patches, designed to rectify security vulnerabilities or system bugs that cyber actors might exploit, also emerged as a prevalent software vulnerability in many systems applications. Respondent R-ICT1 elaborated on this issue, highlighting that when these patches aren't promptly applied following their release, it creates a window of opportunity for cyber actors to exploit vulnerabilities before the necessary fixes are implemented. The respondent also underscored a challenge stemming from obsolete servers within the organisation, stating that the outdated servers often lack up-to-date security controls and measures, exacerbating vulnerability.

Respondent R-ICTM highlighted that the organisation relies on ICT officers who are seconded from the Ministry of ICT. This arrangement partly contributes to vulnerabilities at the organisation, as it has no dedicated ICT department. The respondent narrated:

> *The absence of an in-house ICT department at the organisation has played a role in the vulnerabilities experienced by the organisation.* (R-ICTM)

The findings underscore the observations by Kimani (2023), who reveals a prevailing deficit in organisations regarding the continuity and enforcement of cybersecurity training. He argues that many organisations adopt an "install-and-forget" mentality, neglecting the critical aspects of follow-up and reinforcement of cybersecurity best practices essential for maintaining a strong security posture. Kokkonen et al. (2023) support the observation, asserting that while the initial training provides a foundational understanding of cybersecurity best practices, the ever-evolving nature of cyber threats necessitates continuous education and awareness. Without follow-up cybersecurity training, employees may become complacent or unaware of new risks and attack vectors. This leaves organisations vulnerable to cyber attacks. Regular training sessions and updates are essential for empowering staff to effectively recognise, respond to, and mitigate evolving threats, ultimately strengthening an organisation's cybersecurity posture.

Human factors

The interview findings revealed that employees with authorized access to the organisation's systems, network, or data frequently misuse their privileged access to cause harm to the organisation's security, operations, or data, intentionally or unintentionally. Respondent R-ICT2 narrated:

> *Some officers from the organisation abuse their access privileges to undermine the system, primarily for financial gain. This is a risky move because it could help criminals or other cyber actors steal data and information from the system.* (R-ICT2)

Respondent R-ICTM agreed with Respondent R-ICT2's sentiments, emphasizing the difficulty in detecting insider threats as they are legitimate system users. The respondent narrated:

> *Intentional or unintentional data breaches and sensitive information leakage by system users' employees or contractors are dangerous because they are challenging to detect due to the legitimate access users have. As a result, they may use their knowledge and access to facilitate cyber espionage activities.* (R-ICTM)

According to the respondents, there should be a clear guideline on the level of access that users should have, as they are becoming the primary link to cyber actors. They stated that some officers have access to data and information they should not have access to and may easily collaborate with cyber actors to share and exfiltrate sensitive data.

Some respondent believed that some users ignore installing software or system updates, click on phishing emails that may contain malware, and ignore critical security practices, creating vulnerability for malicious cyber actors to exploit. According to the respondents, the organisation has not invested sufficiently in strict security practices, allowing users to act autonomously.

Insider data breaches are most commonly caused by privilege abuse, with financial gain being the primary motivation. Insiders can also intentionally or unintentionally exfiltrate data for personal gain.

Conclusion

This study examined the cyber espionage vulnerabilities in Kenya's e-Government ecosystem. It revealed that cyber actors constantly probe the target's systems, access controls, and environment to identify and exploit vulnerabilities. These vulnerabilities originate from various sources, such as software flaws, configuration errors, inadequate security controls, or human factors. The exploitation of these vulnerabilities can result in severe and even catastrophic consequences. The study also found that the government's rapid deployment of information technology to enhance service delivery through e-Government systems has not been accompanied by adequate measures to address automation weaknesses and vulnerabilities that could facilitate cyber espionage attacks.

Recommendations

In light of this growing threat landscape, the researcher recommends the following measures for the PI to maintain its cybersecurity posture:

i revise and implement an updated information security policy covering current and emerging cybersecurity issues, addressing access control, data classification, vendor management, password management, and recommended practices and pitfalls;

ii carry out a penetration testing exercise to reveal the true picture of vulnerability;

iii perform a network operations exercise to discover a Cyber-Threat-Intelligence (CTI) based solution for identifying internal and external threats, vulnerabilities, and human factors aiding adversaries, while also addressing cybersecurity skill gaps and compliance with standards;

iv prioritise employee training and awareness by developing comprehensive training programs to educate staff on effective cybersecurity practices;

v implement advanced technologies like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic, detect and block malicious activities, and issue real-time alerts for potential cyber espionage attacks;

vi invest strategically in cybersecurity infrastructure, including antivirus software, firewalls, and modern servers, to proactively safeguard the network and data, blocking and quarantining potential threats; and

vii foster collaboration and information sharing among stakeholders, including private organisations, academia, and other government agencies, to share threat intelligence, best practices, and lessons learned in cybersecurity.

References

Africa Defense Forum. (2022, November 9). Africa Faces High-Tech Enemies. *Africa Defense Forum*. https://adf-magazine.com/2022/11/africa-faces-high-tech-enemies/

Agutu, N. (2016, April 28). Kenya Foreign Affairs ministry emails hacked, sensitive data leaked. *The Star*. https://www.the-star.co.ke/news/2016-04-28-kenya-foreign-affairs-ministry-emails-hacked-sensitive-data-leaked/

Akram, M. S., & Malik, R. (2023). Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security. *Journal of Development and Social Sciences*, *4*(3), 855–864. https://www.ojs.jdss.org.pk/journal/article/view/743

Alderete, M. V. (2018). The mediating role of ICT in the development of open government. *Journal of Global Information Technology Management*, *21*(3), 172–187. https://doi.org/10.1080/1097198X.2018.1498273

Analytica, O. (2021). Microsoft hack will widen US-China rifts on cyber. *Emerald Expert Briefings*, *oxan-db*. https://doi.org.ezproxy.library.strathmore.edu/10.1108/OXAN-DB260397

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences*, *11*(19), Article 19. https://doi.org/10.3390/app11199183

Bello, A., Jahan, S., Farid, F., & Ahamed, F. (2022). A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management. *Water*, *15*(1), 168. https://doi.org/10.3390/w15010168

Carletti, S. (2023, August 1). *Kenya Falls Victim to Cyber-Attack*. IBN Immigration Solutions. https://www.ibn.co.za/blog-and-news/kenya-ecitizen-hacked /

CISA. (2009, May 21). *Choosing and Protecting Passwords*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords

CISA. (2019, September 27). *Understanding Anti-Virus Software | CISA*. https://www.cisa.gov/news-events/news/understanding-anti-virus-software

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

Dilanian, K. (2021, October 7). *Old school spying is obsolete, says one expert. Blame technology*. NBC News. https://www.nbcnews.com/politics/national-security/human-spies-have-become-obsolete-says-one-expert-culprit-technology-n1280965

Douha, N. Y.-R., Sasabe, M., Taenaka, Y., & Kadobayashi, Y. (2023). An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for

Smart-Home Users against Cyberattacks. *Applied Sciences*, *13*(7), Article 7. https://doi.org/10.3390/app13074645

Economic Survey by Kenya National Bureau of Statistics. (2022). https://agrochem.co.ke/2022-economic-survey-by-kenya-national-bureau-of-statistics/

Gov.uk. (2022, December 21). *UK exposes Russian spy agency behind cyber incidents*. GOV.UK. https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents

Herrmann, D. (2019). Cyber Espionage and Cyber Defence. *Information Technology for Peace and Security*, 83–106. https://doi.org/10.1007/978-3-658-25652-4_5

Janczewski, L., & Colarik, A. (2007). *Cyber warfare and cyber terrorism*. IGI Global.

Kimathi, B. (2023, May 15). *The Role of Employee Training in Cybersecurity Risk Management*. https://www.linkedin.com/pulse/role-employee-training-cybersecurity-risk-management-brian-kimathi

Kokkonen, T., Päijänen, J., & Sipola, T. (2023). *Multi-National Cyber Security Exercise, Case Flagship 2* [ACM]. http://www.theseus.fi/handle/10024/797691

Lei, C., Zhang, H.-Q., Tan, J.-L., Zhang, Y.-C., & Liu, X.-H. (2018). Moving Target Defense Techniques: A Survey. *Security and Communication Networks*, *2018*, 1–6. https://doi.org/10.1155/2018/3759626

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Luiijf, E. (2012). Understanding Cyber Threats and Vulnerabilities. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (pp. 52–67). Springer. https://doi.org/10.1007/978-3-642-28920-0_4

Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of e-Government: An integrated conceptual framework. *Technological Forecasting and Social Change*, *173*, 121102. https://doi.org/10.1016/j.techfore.2021.121102

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021). A tale of two cybers—How threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, *18*(1), 1–20. https://doi.org/10.1080/19331681.2020.1776658

Mungai, A. N. (2017). E-Government Strategy Implementation and Performance of the Public Sector in Kenya. *International Academic Journal of Human Resource and Business Administration*, *2*(3). https://www.iajournals.org/articles/iajhrba_v2_i3_301_338.pdf

Nakashima, E. (2015, December 2). Chinese government has arrested hackers it says breached OPM database. *The Washington Post*. https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html

Nyonje, R., Wairiuko, J., & Opiyo, E. (2018). *ICT Infrastructure and Adoption of E-government for Improved Service Delivery in Kajiado County, Kenya*. *10*, 205–221.

Onyando, W. (2023, August 13). *Why spyware attacks are increasing in Kenya*. Business Daily. https://www.businessdailyafrica.com/bd/corporate/technology/why-spyware-attacks-are-increasing-in-kenya--4334792

Patil, A. P., Bharath, S., & Annigeri, N. M. (2018). Applications of Game Theory for Cyber Security System: A Survey. *International Journal of Applied Engineering Research*, *13*(17), 12987–12990.

Pătraşcu, A., & Simion, E. (2013). Game theory in cyber security defence. *Proceedings of the International Conference on ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE-ECAI-2013*, 1–6.

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Applied Sciences*, *12*(3), Article 3. https://doi.org/10.3390/app12031076

Pun, D. (2017). Rethinking espionage in the modern era. *Chi. J. Int'l L.*, *18*, 353. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/cjil18&section=14

Reuters. (2018, January 30). China rejects claim it bugged headquarters it built for African Union. *The Guardian*. https://www.theguardian.com/world/2018/jan/30/china-african-union-headquarters-bugging-spying

Rouse, G. (2022, May 31). *What Is a Firewall and Why Is it Important in Cyber Security?*https://www.datto.com/blog/what-is-a-firewall-and-why-is-it-important-in-cyber-security?utm_medium=opengraph&utm_source=225

Rubenstein, D. (2014). Nation state cyber espionage and its impacts. *Dept. of ComputerScience and Engineering WUSTL, Saint Louis*. https://classes.engineering.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552

Samme-Nlar, T. (2023). *Confronting Africa's Evolving Cyber Threats*.

Sang, M. (2022). *An Appraisal of Kenya's National Cybersecurity Strategy 2022: A Comparative Perspective: 10*.

Shah, H., & Comissiong, D. M. G. (2021). Computer Virus Model with Stealth Viruses and Antivirus Renewal in a Network with Fast Infectors. *SN Computer Science*, *2*(5), 1–8. https://doi.org/10.1007/s42979-021-00780-9

Shepherd, T. (2022, September 30). The biggest hack in history: Australians scramble to change passports and driver licences after Optus telco data debacle. *The Guardian*. https://www.theguardian.com/business/2022/oct/01/optus-data-hack-australians-scramble-to-change-passports-and-driver-licences-after-telco-data-debacle

Thompson, H. H., Whittaker, J. A., & Mottay, F. E. (2002). Software security vulnerability testing in hostile environments. *Proceedings of the 2002 ACM Symposium on Applied Computing*, 260–264. https://doi.org/10.1145/508791.508844

Vandyck, C. K. (2023, July 29). *Strengthening Cybersecurity in Africa: A Call to Action for Governments, Civil Society, and the Private Sector*. https://www.linkedin.com/pulse/opinion-strengthening-cybersecurity-africa-call-action-vandyck

Velluet, Q. (2023, July 5). *Cyberattacks: Five reasons why Africa is vulnerable*. The Africa Report.Com. https://www.theafricareport.com/314687/cyberattacks-five-reasons-why-africa-is-vulnerable/

Verizon. (2020). *2020 Cyber-Espionage Report (CER).* Verizon Business. https://www.verizon.com/business/resources/reports/cyber-espionage-report/

Verizon. (2022). *2022 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Waag-Cowling, N. A. and N. van der. (2021, July 15). How African states can tackle state-backed cyber threats. *Brookings*. https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

Wamoto, F. O. (2015). E-government Implementation in Kenya, an evaluation of Factors hindering or promoting e-government successful implementation. *International Journal of Computer Applications Technology and Research*, *4*(12), 906–915. https://doi.org/10.7753/IJCATR0412.1006

Wanjala, K. (2023, April 13). *Kenya Airports Authority suffers data breach from notorious hacking group*. TechArena. https://www.techarena.co.ke/2023/04/13/kenya-airports-authority-suffers-data-breach-from-notorious-hacking-group/

Welle, D. (2022, February 9). Explained: Why Africa embraces Huawei tech despite security concerns. *Frontline: India’s National Magazine*. https://frontline.thehindu.com/dispatches/explained-why-africa-embraces-huawei-tech-despite-security-concerns/article65220336.ece

Xu, Y., Tran, D., Tian, Y., & Alemzadeh, H. (2019). Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices. *2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. https://doi.org/10.1109/CHASE48038.2019.00017