The Current State of Malware Threats in a Kenyan County Government: A Case Study of Homa Bay County

Okura Odhiambo James

Great Lakes University Kisumu

DOI: https://doi.org/10.47772/IJRISS.2026.101000307

Received: 19 October 2026; Accepted: 24 October 2026; Published: 02 November 2026

ABSTRACT

County governments in Kenya increasingly depend on information systems to deliver public services and malware is a serious threat to those systems. One objective of a thesis on the effectiveness of anti-malware systems in Homa Bay County Government was to describe the current state of malware threats. Single-case mixed methods design was used. Structured questionnaires were sent to 150 employees (136 returned; 90.7%), four ICT key informants were interviewed, logs from [12/14] systems over six months were audited. Questionnaire and audit data were descriptively analysed; interview data thematically. Respondents reported frequent (26.5%) or constant (11.8%) encounters with malware (total 38.2%); none reported (7.4%). Viruses (82.4%), worms (72.1%), Trojans (61.8%) and phishing related threats (55.9%) were most frequently reported followed by spyware (45.6%) and ransomware (27.9%). E-mail attachments and links (76.5%) and removable storage (63.2%) were most often named as sources of infection. Mean self-rated malware knowledge was 3.44 out of 5. Key informants said incidents cleaned silently by the software were not always reported. In six months the audit recorded 24 malware incidents: 20 (83.3%) were automatically resolved; four needed manual intervention; two were repeated phishing detections. Malware was widely perceived as a regular threat in this County Government, respondents and informants identified e-mail and removable media as entry points and informants said incidents were underreported when silently resolved. The study is one county and combines self-reports with a limited log audit so results are descriptive and cannot be generalised statistically. Awareness and phishing resilience training should continue, removable media controls enforced, incident reporting mandatory, centralised log monitoring implemented and national threat intelligence sharing encouraged.

Keywords: county government; phishing; infection vectors; cybersecurity; Homa Bay County; Kenya

INTRODUCTION

Background to the Study

Malware is referred to any type of software designed with the purpose of causing damage to a computer system, server, client, and network including viruses, worms, Trojan horses, ransomware, spyware, adware and file less malware (Kaspersky Lab, 2024). Malicious programs exploit vulnerabilities in information systems in order to access confidential information, cause disruption in their operations, request extortion, or create a backdoor to future incursion. Modern malware uses advanced techniques such as polymorphism, metamorphism and encryption, which enables many cyber criminals to bypass signature based detection (Savenko et al., 2022). Hence, organizations around the globe face highly capable attackers, who may be government institutions, because of the volatile nature of the data and the extent of the disruptions they can cause.

According to the World Economic Forum's Global Risks Report (2024), cyberattacks rank among the top five global risks for the next decade, with critical infrastructure and government being main targets. The International Telecommunication Union's Global Cybersecurity Index (2023) shows that approximately 78 percent of the nations have developed national cybersecurity strategies, but there are still major gaps in implementation especially in developing countries. While the Convention on Cybercrime by the Council of

Europe fostered international collaboration, the transnational nature of cyber threats continues to outpace regulation (United Nations, 2023).

The recent high-profile incidents in developed nations such as Colonial Pipeline ransomware attack in the United States, the WannaCry ransomware attack of the United Kingdom National Health Service, and the NotPetya attacks on the Ukraine government systems are clear examples of global vulnerability in which even advanced nations have difficulties protecting themselves from cyber threats (Kshetri & Voas, 2023). Altogether, the above statements point out the international challenge of protection of governmental information systems from malware attacks that take place on the increasing scale.

In the context of Africa, peculiarities of the cybersecurity situation are determined by fast digitalization, unevenly developed infrastructure and low institutional capacity. During the last decade Africa has seen the significant increase in the number of internet users with more than 570 million people being connected in 2023 which is 40 percent higher compared to 2020 (Internet World Stats, 2024). This leap forward has brought considerable socio-economic benefits but has increased at the same time the threat surface accessible for criminals. The Malabo Convention on Cyber Security and Personal Data Protection by the African Union establishes the continent in a frame work for harmonization of cybersecurity policies; however, the ratification and implementation of this convention varies greatly in member states (African Union, 2023).

The Africa Cybersecurity Report (2023) shows that the government agencies all over the continent experience on average 1,500 attempts to attack cyber infrastructure weekly, malware being responsible for 62 percent of successful incursions. South Africa, Nigeria and Kenya are considered as main targets because of the advanced digital economy in these countries, while countries with underdeveloped digitized infrastructure are faced with problems in detecting or reacting to emerging threats (Serianu, 2023). The Interpol Africa Cyber Threat Assessment Report (2024) mentions the ransomware attacks, banking Trojans, and the compromise of business email as prevailing threats to the governments of contemporary Africa. This is additionally complicated by the lack of technical expertise, limited security budget and weak cyber defences.

In Kenya, the wide-spread digital transformation program makes ICT the core of national development strategy and demonstrates the direction towards integration of technologies. Programs such as the Digital Economy Blueprint, the Huduma Kenya programme, and e-Citizen show the efforts made by the Ministry of ICT and Digital Economy in the centralization of government services and the digitization of extensive amounts of data belonging to the citizens (Ministry of ICT, 2023). The Communications Authority of Kenya reports more than 1.2 billion cyber-threat events in the fiscal year 2023/2024, which is 35 percent higher compared to the previous year, 400 million of them being related to the malware (Communications Authority of Kenya, 2024).

While the decentralization of ICT infrastructure is not accompanied by corresponding investments in security. According to the analysis carried out by the Kenya National Audit Office (2023), 68 percent of county governments do not have the cyber security directives at all, 72 percent are inadequate in the reaction to incidents, and 83 percent have annual malware attacks on the critical systems. Homa Bay County Government, located in the western part of Kenya at the shore of Lake Victoria, serves as a perfect example of this situation: the county provides services in the eight sub-counties in health, financial, educational, agricultural and ICT fields, hence managing sensitive information from the patients' records to the financial and personnel data (Homa Bay County Government, 2024). Malware attacks that are happening repeatedly affect the operations, the integrity of the data and raise the concerns among the citizens of the leakage of their personal information (Njenga, 2023). The study is based on three related theories. The independent variables include threats by malware (varieties, number, intensity, origin) and technological defences (signature-based detection, heuristic analysis, behaviour-based monitoring, AI-based security solutions). The dependent variable is the effectiveness of anti-malware systems, measured through detection rate, mitigations accomplished, resilience of the system throughout its lifecycle, and the user satisfaction. Organizational characteristics mediate the relation between technologies used and security results.

The theoretical background consists of Protection Motivation Theory (Rogers, 1975), which connects the threat perception with coping appraisal and security behaviour; Technology Acceptance Model (Davis, 1989) that highlights the importance of the usefulness and ease of use of the technology in the process of adoption; and General Deterrence Theory (Gibbs, 1975) that says that the awareness of the threat consequences leads to the compliance with the security procedures. Substantial empirical literature exists on the evolution of malware threats and the effectiveness of the corresponding countermeasures. Internationally, Al-Duwairi and Al-Eroud (2021) performed a wide research of the tendencies of the malware evolution including polymorphic and metamorphic varieties that bypass the signature-based detection.

The authors prove that the behaviour- and AI-based defences are crucial for staying ahead of emerging threats. Ahmad and Khan (2021) conducted a similar research of the global malware trends that reveal that ransomware and APTs increasingly target the government systems, attack sophistication outgrowing the defensive capabilities. Chukwuma (2022) studied the challenges that cybersecurity faces in government institutions in Africa pointing out the lack of infrastructure, the skills shortages, and limited funding as the main obstacles for effective malware protection. Adeyemi (2022) studied the anti-malware measures in public sector organizations in Africa and found that many of them use primitive tools and lack the defence against sophisticated threats. Wanjiku (2023) evaluated the malware threats to county governments in Kenya showing that outdated systems, inconsistency in updating and poor user awareness lead to persistent vulnerabilities.

Empirically, there is little recent and localized data on the number and results of the malware attacks in Kenyan county governments after the adoption and implementation of the National Cybersecurity Strategy 2022-2027. These gaps prove the necessity of the targeted research that would provide the context-specific evidence. The situation described above justifies the evaluation of anti-malware systems in the county governments of Kenya. Despite the efforts that have been undertaken by the country for improvement of cybersecurity, the county institutions still face malware threats, both old and emerging, as the literature suggests. For example, the Homa Bay County Government in Kenya demonstrates the complex conditions in which the devolved institutions have to deliver digitized services while protecting the sensitive information from advanced cyber threats.

Taking into account the combination of global trends of the threats, local capacities, barriers to policy implementation and reality on the ground, systematic inquiry is justified in this case. In this context, the current study aims to provide the empirical data on the effectiveness of anti-malware systems in Homa Bay County Government with the goal to contribute to cybersecurity improvement in the devolved governance of Kenya.

The presence of anti-malware systems in the organization does not mean automatic protection of the information systems. The effectiveness of such system depends on its capability to detect the malicious software, prevent its execution, facilitate remediation, keep up with the emerging threats, and operate effectively in the organizational environment. Thus, the assessment of the anti-malware effectiveness implies the consideration of the technical performance and organizational factors such as staff expertise, cybersecurity awareness, patch management, policy implementation and resources availability. This distinction is especially important in the case of county governments in which the protection of information systems depends not only on the technologies employed but also on their configuration, maintenance, and usage.

This study provides an empirical depiction of the malware threat environment in the Homa Bay County Government, a neglected area in the cyber security literature of the African public sector. The study can be used as a benchmark to measure any changes in the future through conducting other studies in Homa Bay and other counties. For Homa Bay County Government, the study will identify malware types, infection vectors, and reporting issues that should be addressed when planning for the cyber security. For policymakers, including Ministry of ICT and the Communications Authority of Kenya, the study will give county-level evidence on the implementation of the National Cybersecurity Strategy 2022–2027. For researchers, the study shows the usefulness of triangulating survey perception data with interview evidence and technical logs to describe organizational threat exposure.

Problem Statement

Despite the use of different anti-malware products in the county governments in Kenya, the ongoing and recurrent attacks by malware pose a threat to the integrity and confidentiality of critical information systems, making one wonder about the overall effectiveness of the cybersecurity measures employed by the counties. For instance, the preliminary and anecdotal evidence about the Homa Bay County Government shows that malware infections often bypass the current defences leading to the system downtime, data corruption, and unauthorized access to government files (Njenga, 2023). The Communications Authority of Kenya (2024) reported 400,000 malware attacks in county governments in the fiscal year 2023/2024 with 28 percent of attacks being successful and compromising the systems.

The ICT audit conducted by the Kenya National Audit Office (2023) in 47 counties showed that 76 percent of them had experienced at least one serious malware-related security breach in the preceding two years, national financial losses totalling KES 2.3 billion. Specifically, for Homa Bay County, the records of the ICT department of the county show that there were 147 malware incidents between January 2023 and June 2024, including ransomware infections, which resulted in temporary restriction to access to health records, spyware infections compromising the personnel data, and Trojan infections affecting the financial transactions system (Homa Bay County ICT Department, 2024). Also, the preliminary results of this study reveal that 34 percent of employees in the county government reported their exposure to malware, with the technical analysis uncovering such issues as lack of regular patches and the legacy of the signature-based detection systems.

Overall, the data collected proves that the malware is a tangible and quantifiable threat to the information systems of Homa Bay County Government. It goes beyond the technical aspect involving the substantial operational, financial and social implications. Operationally, the attacks caused the system outages and disrupted service delivery, including delaying of salary payments, problems in management of health patient records, and access to the agricultural extension data needed by the local farmers (Odhiambo & Mwangi, 2023). The Homa Bay County Treasury (2024) reported the emergency cybersecurity expenses of KES 8.7 million in the 2023/2024 fiscal year. Socially, the ongoing security incidents decreased the trust in the county government's ability to protect citizen data, with 63 percent of the Homa Bay population being worried about the safety of their personal information stored in government systems (Wanjiku, 2023).

The discrepancy between policy implementation and its performance calls for careful evaluation in order to understand the reasons behind the failure of the current cybersecurity measures. Despite the growing literature on the topic of cybersecurity in the public sector, several major research gaps exist, which the study is aimed to close. While the international research evaluated the malware threats to the government of the developed countries (Al-Duwairi & Al-Eroud, 2021; Ahmad & Khan, 2021) and continental researches revealed the challenges to the cybersecurity in the public sector of Africa (Adeyemi, 2022; Chukwuma, 2022), there is little empirical research examining the effectiveness of the anti-malware systems in Homa Bay County Government.

Wanjiku (2023) investigated the malware threats within Kenyan counties but mainly addressed the prevalence of the threat instead of providing the detailed empirical evaluation of the countermeasure effectiveness. Njenga (2023) investigated the anti-malware systems in Kisumu County and provided the substantial information about the problem; however, the results of this research are not easily comparable to the results for Homa Bay because of the different conditions of infrastructure, capacity and threat exposure. Methodologically, the literature was mainly based on either quantitative survey or qualitative interviews, while the approach combining both methods and the triangulation of the perceptual data and the audit of the technical system was used in order to evaluate anti-malware effectiveness as an objective measure.

This article is focused on the first dimension of the problem, namely on the nature and scale of malware threats that the county's anti-malware systems are supposed to counter. In the absence of the contemporary and complete description of the malware varieties, frequency and sources, it is impossible to determine if the current defences are aligned with the threats. Previous studies were mainly based on the perceptual data or

national and multi-county statistics, and few studies triangulated the experiences of the employees, key informants and system logs in order to characterize the threat environment of a single county government.

Objectives of the Study

an environment would provide specific evidence of the interactions between technical controls, human factors, and organizational capabilities. There is a justification for the research since it will provide current, local, and triangulated evidence on the malware threats facing the devolved government. National statistics can help in knowing the extent of the challenge, but cannot tell us which kinds of malware threats the county staff face, what channels do the threats come via, and whether they detect all the threats. The research will provide a more detailed picture of the threat environment in Homa Bay County through integration of survey data, interviews and system logs. The description of the threat environment would serve as the basis for evaluating the effectiveness of the anti-malware tools.

Main Objective

The main objective of the study was to evaluate the effectiveness of anti-malware systems in Homa Bay County, Kenya. This article seeks to answer one specific objective of the overarching study.

Specific Objective of this article:

To assess the current state of malware threats faced by the Homa Bay County Government.

Research Question

What kinds of malware threats are prevalent in the Homa Bay County Government, what is the frequency of encountering these threats, and what channels do these threats come through?

Scope and Delimitation

This study will focus on the Homa Bay County Government, Kenya and the effectiveness of the anti-malware systems in use. The study will evaluate the malware threats encountered, will assess the technologies in use, will identify the gaps and challenges that affect the effectiveness of antimalware systems and will obtain input from information technology staff and other employees. Geographically, the scope is limited to activities in Homa Bay County only; no other counties or national agencies will be studied. Contextually, the study will focus on the government offices and the information technology infrastructure of the county. Data gathering and technical assessment will take place within a particular time frame (such as three months).
The delimitation of the scope of the study will make it manageable and consistent with the stated objectives. Private sector networks, non-governmental organizations, and individuals are excluded. Firewalls, intrusion detection systems and physical security will not be assessed; the focus is on the anti-malware solutions.

The study will exclude any in-depth forensic investigation of previous cybersecurity incidents. Interview and survey respondents will include only current employees and IT staff of Homa Bay County. This article will focus on one objective, namely the current state of malware threats, and provides evidence gathered through questionnaire, interviews and audit of system logs related to that objective.

LITERATURE REVIEW

Theoretical Framework

The theoretical framework helps guide the examination of variables, relationships, and findings (Creswell & Creswell, 2021). This study uses the following theoretical frameworks: Protection Motivation Theory (PMT), General Deterrence Theory (GDT), and Technology Acceptance Model (TAM).

Protection Motivation Theory

Rogers (1975) developed Protection Motivation Theory (PMT). PMT describes how people appraise threats and take protective action: threat appraisal (severity and vulnerability perception); coping appraisal (response efficacy, self-efficacy and cost of response) (Rogers, 1983). Protection is more likely when people believe a response is effective, feel capable of applying it and think costs are manageable. PMT explains how threat perceptions and confidence in anti-malware systems affect compliance and reporting. Threat and coping appraisals predict protective behaviour (Ifinedo, 2012; Boss et al., 2015) although PMT may overstate institutional, cultural, habitual and social influences (Posey et al., 2015).

General Deterrence Theory. GDT states that violations are discouraged by the certainty, severity and speed of sanctions (Gibbs, 1975). In information security it explains compliance with security and acceptable-use policies (D'Arcy et al., 2009; Herath & Rao, 2009). Employees may avoid malicious links, unauthorized devices or disabling security software when they expect detection and sanctions. Security-rule awareness, surveillance and sanctions can help support compliance (D'Arcy et al., 2009; Herath & Rao, 2009). However GDT overlooks ethical, organizational and habitual factors and deterrence weakens without monitoring (Siponen & Vance, 2010).

Technology Acceptance Model. TAM explains technology acceptance through perceived usefulness and perceived ease of use (Davis, 1989). Beliefs about anti-malware, authentication and encryption use (Venkatesh & Davis, 2000; Venkatesh et al., 2003) are based on usefulness, ease of use, updating and response to alerts in anti-malware tools. Employees may judge anti-malware tools by usefulness, ease of use, updating and response to alerts. Inconvenient software can be ignored or disabled. Perceived usefulness and ease of use predict technology use (Venkatesh et al., 2003) and intentions to use anti-malware solutions (Ng & Rahim, 2005). TAM ignores emotional, social and moral influences (Bagozzi, 2007). Integration of theories and connection to study variables PMT explains threat appraisal and protective motivation, GDT policies, monitoring and sanctions TAM usefulness and ease of use so effectiveness depends on awareness (employee), policy enforcement (technology) software usability as well as technology.

Empirical Literature

Threats to Organizations from Malware

Al-Duwairi and Al-Eroud (2021) reviewed over 200 publications between 2015–2020 and found increasingly sophisticated malware such as polymorphic/metamorphic forms, memory based activity evasion of signature detection and ransomware-as-a-service. Ahmad and Khan (2021) describe advanced persistent threats using social engineering, zero-day exploitation and customised malware and advocate behavioural and AI-based detection. In Sub-Saharan Africa, Chukwuma (2022) surveyed 187 ICT directors and security personnel in 15 countries: 78% of government organisations had a successful infection within the past year. Ransomware, phishing and botnets were common; estimated losses $250k; weak infrastructure, skills shortages, budgets and employee awareness made them vulnerable. National cybersecurity strategies and incident response teams reduced infections and recovery time. Adeyemi (2022) interviewed 45 ICT managers in Nigeria, Ghana, Kenya and South Africa to show that budget and procurement constraints forced basic antivirus use (only 22% of institutions used advanced endpoint detection and response); late updates, inconsistent patch management and poor integration were common.

In Kenya Wanjiku (2023) studied Homa Bay, Kisumu and Mombasa counties using 342 employee surveys, interviews and incident reports: Sixty-seven per cent reported infections in the previous year: viruses (82%), phishing-related Trojans (71%), ransomware (43%) and spyware (38%). Incidents caused data and financial losses with an average downtime of 4.7 days. Old software was used; training was inadequate; ICT personnel were insufficient. Njenga (2023) studied Kisumu County Government using 45 technical audits, 112 employee surveys and ICT interviews. Signature databases were out of date in 34% of systems; full-system scans were not scheduled in 28%; 42% of threats required manual intervention; departments with recent security training had 47% fewer successful infections.

Author (Year)	Key Findings	Identified Research Gap
Al-Duwairi & Al-Eroud (2021)	Malware increasingly uses polymorphic, metamorphic and fileless techniques to evade signature-based detection; ransomware-as-a-service has lowered the entry barrier for cybercriminals.	Relies on published literature rather than primary data; limited representation of developing-country contexts.
Ahmad & Khan (2021)	Government institutions are prime targets for advanced persistent threat groups using multi-stage attacks; signature-based detection is becoming inadequate.	Focused on high-profile attacks in industrialized countries; excluded African and developing-nation contexts.
Chukwuma (2022)	78% of African government organizations experienced successful malware infections; drivers include poor infrastructure, skills gaps and low user awareness.	Self-reported data subject to recall and desirability bias; continental overview misses country-specific nuances.
Wanjiku (2023)	67% of Kenyan county governments experienced malware infections; viruses (82%), phishing Trojans (71%) and ransomware (43%) most prevalent; average downtime 4.7 days per incident.	Reliance on employee recall for incident reporting; inconsistent record keeping across counties.

Table 2.1: Summary of Literature Reviewed on Malware Threats

Conceptual Framework

The conceptual framework described in this article captures the definition of the threat environment for the malware threats in the County, as well as the elements that influence this environment. The threat environment, which is the basis of the first objective, is defined by the prevalence and occurrence of malware, the diversity of malware seen, the means of transmission used, and the incidents reported. It is influenced by the user's awareness and behaviour (PMT), by the policy and reporting environment (GDT), and by the protective technology (TAM). This is captured in the table below.

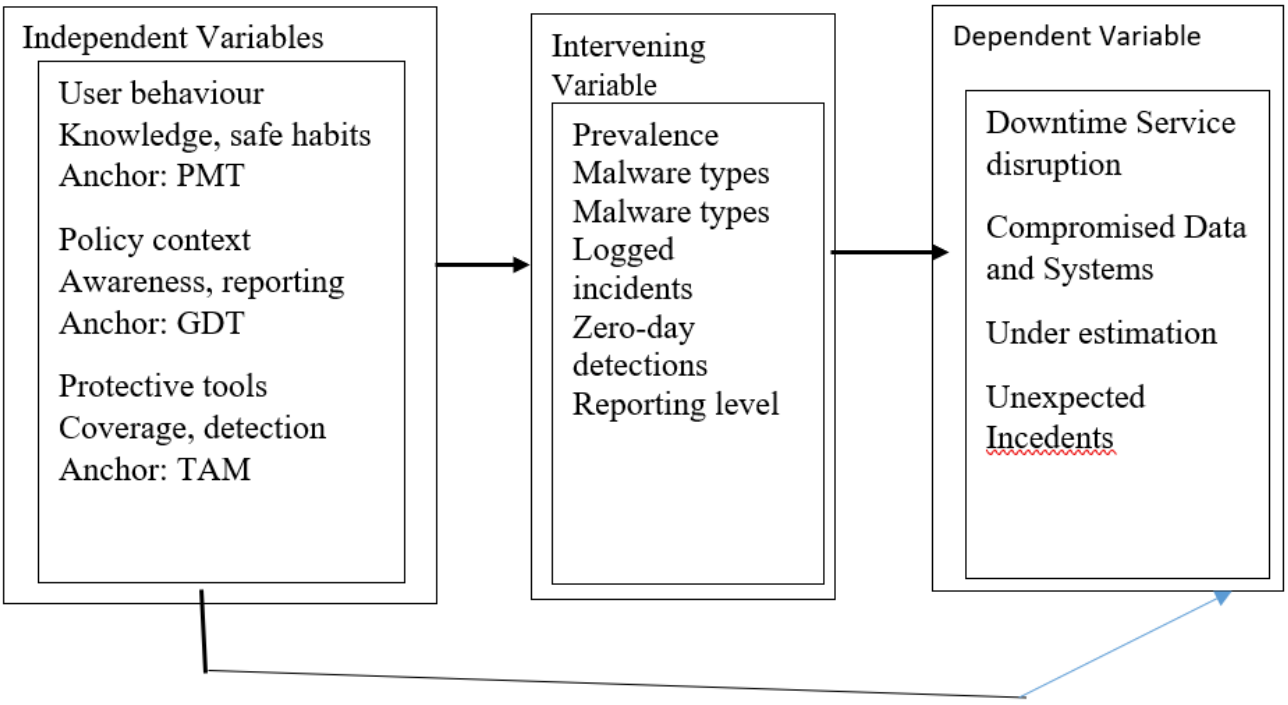

Fig 2.1: Conceptual Framework for the Current State of Malware

Theoretical Base

The conceptual framework is based on Protection Motivation Theory (Rogers, 1975) that shows how perceived threat severity and vulnerability influence protective behaviour; General Deterrence Theory (Gibbs, 1975) which looks at policy awareness and consequences influencing compliance and reporting; Technology Acceptance Model (Davis, 1989) which shows how perceived usefulness and usability affect security technology acceptance. Taken together these theories imply that organizational malware threats are shaped by interaction between technical exposure, human behaviour and organisational practices.

Assumptions of the framework

Variables are measurable (through surveys, interviews and technical audits) so valid and reliable data is produced; independent and dependent variables are mainly linear while external influences are relatively stable; respondents are assumed to be aware and recall information well enough; infrastructure (e.g. organisation), staffing, security policies and anti-malware systems remain representative and relatively constant throughout data collection; causal relationships go from independent variable through intervening variable to dependent variable.

RESEARCH METHODOLOGY

Research Design

In order to analyse anti-malware systems based on measurable and contextual information, the case study with mixed methods design was used. The quantitative data were collected using structured questionnaires to examine employees' perceptions, experience, and reported security behaviours. Qualitative data were collected via semi-structured interviews with ICT key informants and technical system audits.

This design is appropriate for studying the ICT infrastructure and people working in it within the authentic context (Yin, 2018). The use of triangulation of responses to questionnaires, interview data and results of the technical audit increased credibility and reliability of the findings (Creswell & Poth, 2018; Denzin, 1978; Patton, 2015). This made it possible to combine technical issues, perceptions of the users and organizational conditions and identify the cybersecurity problems that could not be identified using just one methodology.

Study Site/Study Site Description

The Homa Bay County is located in western Kenya on the shore of Lake Victoria, sharing borders with Kisumu County to the east, Kericho County to the southeast, Migori County to the south, and Siaya County to the west. The administrative center is in the town of Homa Bay. According to the Kenya National Bureau of Statistics (2022), the population of the county is about 1.2 million people, and it manages such departments as administration, health, agriculture, ICT, finance, education, and municipal services.

The ICT department manages roughly 1,200 network devices, including desktop computers, laptops, servers, and network equipment in the headquarters and sub-county offices. Homa Bay County was selected for the study because of malware incidents reported in its systems (Homa Bay County ICT Department, 2024; Njenga, 2023) and its status as an example of the devolved government entity with resource limitations typical for Kenyan county governments.

Target Population

The target population is comprised of employees using the ICT systems of Homa Bay County Government during their work. There are two categories: ICT employees of the county: There are 28 ICT employees in the ICT department including the Head of ICT, two system administrators, three network engineers, one cybersecurity officer and 21 support and technical staff. These employees are responsible for installing, configuring, monitoring and maintenance of the anti-malware systems and have specific knowledge that can help to evaluate their operational effectiveness.

Non-ICT employees of the county government: This category included administrative staff, financial and accounting officers, HR specialists, records managers, programme assistants, health records officers, and agricultural extension officers. Their experiences helped to evaluate cybersecurity awareness, behavioural factors, and system performance. Human errors and unsafe user behaviour are considered among reasons of cybersecurity threats (Nobles, 2022; Hadlington, 2021). The number of ICT users in the selected departments, according to the records of the county human resources department confirmed by the ICT department, was about 1,200. These employees became the sampling frame.

Sampling Techniques and Sample Size

For gathering the relevant information from technical and non-technical participants the study used both purposive and probability-based sampling (Taherdoost, 2022) Purposive sampling: In order to conduct in-depth interviews, the Head of ICT, two system administrators and one network security officer were selected because of their specific knowledge concerning anti-malware configurations, previous incidents and operational restrictions. Also, 12 systems covering different functions in the ICT, finance and administrative departments were selected for technical audits. Such sampling technique allowed selecting participants and systems containing the information relevant for the study (Palinkas et al., 2015).

Stratified random sampling: The non-ICT employees were selected using stratified random sampling. The population was stratified by departments – health, finance, administration, agriculture, education, and public works. The employees were randomly selected from each stratum to increase representation, minimize selection bias, and capture the differences in exposure to malware and cybersecurity awareness (Thompson, 2012).

Sample Size Estimation

The sample size was estimated in accordance with the social research standards suggesting that 10-20% of accessible population can be enough for regression analysis (Taherdoost, 2022; Hair et al., 2021). From the population of approximately 1,200 ICT users the sample of 150 respondents was set. The regression model included six predictors: staff training, patch management, type of anti-malware technology, user awareness, policy enforcement, and resource allocation. As per the recommendation concerning the minimal number of 10-15 observations per predictor variable needed for statistical power and stability of estimation (Field, 2018), the minimum of 90 respondents was needed. The suggested sample size of 150 exceeded the minimal requirements and was considered sufficient.

Table 3.1: Strata Sampled

Department/Stratum/	Population Estimate	Sample Allocation	Sampling Method
ICT Personnel	28	20	Purposive
Administrative Staff	180	35	Stratified Random
Finance Staff	150	30	Stratified Random
Health Records Staff	200	25	Stratified Random
Agricultural staff	170	20	Stratified Random
Other Departments	472	20	Stratified Random
TOTAL	1200	150	

With the aim of facilitating statistical power, conducting regression analysis, comparing subgroups within departments, and accounting for the expected 15% non-responses, the target sample of 150 respondents was

found to be adequate. As proposed by Fefferman and Sverchkov (2025), selection bias was minimized through a combination of non-probability and probability sampling. Hence, purposive sampling of experts in the subject matter was supplemented with stratified random sampling in order to maximize both depth and breadth. The resulting sample size was 136 respondents, representing a response rate of 90.7% that was attained through follow-ups, departmental visits, and assurance of anonymity. Six variables were used in the multiple-regression analysis: staff training, patch management, type of anti-malware technology, user awareness, policy enforcement, and resource allocation. According to Green (1991), a minimum sample size of 60 respondents was required, whereas Faul et al. (2009) suggest a minimum of 98 respondents for 80% of statistical power, medium effect size, and 5% significance level. Thus, the attained sample size is above minimums.

Four key informants were selected using purposive sampling: Head of ICT, System Administrator, Network Security Officer, and ICT Support Officer. Despite the recommendation by Guest et al. (2020) for 8-12 interviews to reach saturation in similar populations, saturation was determined through transcript reviews, revealing no emergence of any new themes after the fourth interview. Interviews and technical audits conducted within five months have provided contextually grounded findings using triangulation method.

Instruments for Data Collection.

Table 3.2: Operationalization of Variables for Objective One

Variable	Dimensions	Indicators	Measurement	Data Source
Current state of malware threats	Prevalence and frequency	Frequency of malware encounters	Never to constantly (5 categories)	Questionnaire
	Types of malware	Types encountered (virus, worm, Trojan, phishing, spyware, ransomware, adware)	Multiple response; frequency/percentage	Questionnaire; interviews
	Infection vectors	Sources of infection (e-mail, USB, browsing, downloads, network)	Multiple response; frequency/percentage	Questionnaire; interviews
	Documented incidents	Incidents detected, resolved, repeated infections	Counts and percentages from logs	Technical audit (logs)
	Detection of novel threats	Zero-day detections as share of detections	Percentage	Technical audit
	Reporting and awareness	Self-rated malware knowledge; reporting practice	5-point Likert; themes	Questionnaire; interviews

Three complementary data collection instruments were used in this study: a structured questionnaire, a semi-structured interview guide, and a technical audit checklist. All three were developed with the view to collect data concerning the aims of the research, particularly focusing on the frequency and nature of malware threats, malware types, infection routes, log incidents of malware, and ability to detect unknown threats.

Structured Questionnaire

Quantitative data were collected by the questionnaire on employees' knowledge of malware threats, experiences, effectiveness of anti-malware tools, and problems with their implementation. It consisted of six sections: (A) general information about demographics and occupation; (B) knowledge and experience of malware threats; (C) existing anti-malware measures and their perceived effectiveness; (D) implementation gaps in terms of training, budgeting, performance, and updates; (E) recommendations for improvement and confidence in the capability of the county to address the issues; (F) other comments. It predominantly included

closed-ended questions with response options coded to facilitate quantitative analysis but some open-ended questions were included for additional perspectives to be considered. Opinions were measured on a five-point Likert scale for analysis purposes and for convenience of respondents (Fowler, 2014; DeVellis & Thorpe, 2021).

Semi-Structured Interview Guide

Interviews were conducted with ICT and cybersecurity experts to gather qualitative data on their responsibilities, anti-malware tools and reasons for their choice, system configuration, update and scan procedures, history of malware incidents, their detection and response time, challenges related to the implementation, strengths and weaknesses of the systems, and recommendations for improvement. Its flexibility was expected to allow emerging topics to be clarified and investigated while sticking to the goals of the study (Merriam & Tisdell, 2016; Kallio et al., 2016).

Technical Audit Checklist

The technical audit checklist provided a reliable evaluation of the installed anti-malware systems and addressed the drawbacks of the use of only perceptual data (Wanjiku, 2023; Njenga, 2023). It included seven sections: system information and licensing; configuration (real-time protection, automatic updates and scans); system logs and malware incidents; incident-response; vulnerability scanning and patch management; detection statistics and performance; observations and recommendations of the auditors. It included system inspection, examination of system logs, and discussions with ICT personnel. The evidence-based nature of this tool made possible to conduct a consistent and comprehensive technical assessment (National Institute of Standards and Technology, 2020).

Validity and Reliability of Instruments

To ensure valid and reliable results, the validity and reliability of instruments were assessed (Creswell & Creswell, 2021).

Validity

Content validity was ensured by developing items of the instruments based on the literature on malware threats, effectiveness of anti-malware tools and cybersecurity challenges (Al-Duwairi & Al-Eroud, 2021; Ahmad & Khan, 2021; Wanjiku, 2023). The instruments include items on the components of threat appraisal, coping appraisal, deterrence, and technology acceptance.

The instruments were reviewed by two supervisors in terms of their clarity, relevance, and appropriateness. To test the face validity, the instruments were piloted on 15 participants, including 10 non-IT staff and five IT experts, who identified unclear items through cognitive interviewing. The technical audit checklist was piloted on three systems to examine its usability and completeness. Triangulation ensured construct validity, while factor analysis was going to be performed to determine if the items in the questionnaire loaded on their corresponding scales (Hair et al., 2021).

Reliability

Reliability is the consistency and stability of measurements (DeVellis & Thorpe, 2021). The internal consistency of the items was estimated with Cronbach's alpha, with $\alpha \geq 0.70$ regarded as an acceptable value (Nunnally & Bernstein, 1994; Taber, 2018). In the scales of perceived effectiveness, user awareness, and policy enforcement, Cronbach's alpha was 0.82, 0.78, and 0.75, respectively. Inter-rater reliability was checked when two researchers conducted audit of four systems, and disagreements were resolved through discussion. The test-retest reliability of the questionnaire was tested when it was administered to eight pilot participants twice with two-week interval between the administrations. To ensure reliability, standardized procedures were followed when conducting interviews and questionnaires and performing technical audits

Trustworthiness of Qualitative Elements

Trustworthiness was established based on the criteria proposed by Lincoln and Guba (1985): credibility, transferability, dependability, and confirmability. Credibility was ensured through triangulation, member checking, and peer debriefing with supervisors. Transferability was ensured through providing the detailed description of the study context, participants, and procedures. Dependability was shown by keeping the audit trail. The confirmability was ensured through maintaining the reflexive journal in which the researcher's assumptions and biases were recorded and triangulation.

Data Collection Methods

For data collection on malware threats and the efficiency of anti-malware approaches, the study adopted questionnaires, semi-structured interviews, and technical system audits as data sources.

Table 3.3: Data Sources and Their Contributions

Data Source	Population/Sample	Instrument	Variables Covered	Analysis
Questionnaire	136 county employees	Structured questionnaire (Section B)	Knowledge of malware, frequency, types and sources of malware	Descriptive statistics
Interviews	4 ICT key informants	Semi-structured interview guide	Threat experience, reporting practice, user behaviour	Thematic analysis
Technical audit	12 systems	Audit checklist and system logs	Incidents detected and resolved, repeated infections, zero-day detections	Descriptive

Survey Administration

Questionnaires were distributed to a sample of county employees after being authorized by Homa Bay County Government through an introductory letter from Great Lakes University of Kisumu (see Appendix D). Respondents were identified through contact persons from respective departments. All the questionnaires had a cover letter indicating the purposes, importance, and assurance of confidentiality of the study.

The respondents were given the option of completing the questionnaires either on site or within two to three days. The follow up involved collecting the completed questionnaires and clarifying ambiguous questions. Those who opted to participate electronically got the questionnaires through Google forms through emails. The mixed approach of administration ensured consistency while considering individual preferences (de Leeuw, 2018). The distribution and collection led to a response rate of 90.7% equating to 136 out of 150 distributed questionnaires.

Interviews with Key Informants

Purposive four key informants consisting of the Head of ICT, two system administrators, and a network security officer participated in the semi-structured interviews due to their expertise on the topic under study. Interviews were conducted in convenient places, which were mainly in county offices for about 45 to 75 minutes. After getting informed consent, interviews were audio recorded and accompanied by notes in case of nonverbal aspects and contexts. The flexible semi-structured interviews guided the discussions for exploring emerging themes. Summaries from previous interviews informed the upcoming ones while transcriptions of interviews were done verbatim within 48 hours.

Technical System Audit

A technical audit was conducted in collaboration with ICT department over a 14-day period. Twelve systems were purposively selected from ICT department, finance department, and administrative departments. These consisted of two servers, a domain controller, and a file server and ten workstations. The audits were scheduled at low activity times to avoid disruption. With authorization, system administrators gave the authorized access. Real-time protection, automatic update, scan schedule, and advanced detection settings were assessed through system interfaces and configuration files.

Logs from the last six months were reviewed to establish the number of malware detections, automated and manual responses, false positives, and recurrent infections. Updates of operating system and third party applications, vulnerability scan reports, and patches compliance were reviewed. Detection statistics from anti-malware console were compared with the independent scans where possible. Security policies, incident-response plans, and other documents were reviewed. Observations were done using an audit checklist and with authorized photographs as the evidence. The findings were discussed with the ICT staff to ensure their correctness.

Triangulation was used for combining employee survey, expert interviews, and technical audits in order to combine the perspective of the whole workforce with the expert knowledge and technical systems audit evidence. Ethical guidelines were followed throughout the research.

Ethical Considerations

Ethical clearance was sought from the Ethics Review Committee of Great Lakes University of Kisumu and a research license was acquired from NACOSTI (see Appendix C).

Informed Consent

The participants were given the information explaining the study's aims, procedure, risk and benefits, confidentiality measures and their rights. Participation in the survey was optional and the questionnaire submission amounted to informed consent. The participants for interviews got the consent forms and signed them after discussion. The participants were informed of their right to withdraw without any penalties.

Confidentiality and Anonymity

For survey respondents, they were not required to provide names. Interview participants were assigned pseudonyms and identification details were omitted in the transcripts and reports. The paper records were kept in locked cabinets while electronic records were password protected and encrypted. Only the researcher and supervisors had the access to them. The findings were reported using aggregate data and anonymous quotes.

Consent, Organization, and Access

Informed consent was acquired from Homa Bay County Government by submitting an introductory letter and a research proposal to the County Secretary and Chief Officer for ICT (see Appendices D and E). Data collection was scheduled to accommodate staff responsibilities and minimize the operational disruption. Auditing entailed the observation of the existing configuration and logs and no penetration testing and vulnerability exploits were conducted.

Data Security and Privacy

System logs and configurations were considered sensitive data. They were secured, and the identifying information, IP address and system name were omitted during processing. The findings were reported in aggregate form to prevent the disclosure of the system vulnerabilities.

Limitations of the Study

There were some limitations faced in this study. First, the limitation of the single case design makes the statistical generalizability difficult for other counties, although the contextual findings may inform similar settings (Yin, 2018). Second, the cross-sectional design cannot make causal inferences. Third, auditing 12 out of around 1,200 devices offers the indicative but not comprehensive evidence.

Fourth, there may be some biases in the self-report data, as well as technical records and configurations, such as recall and social desirability. Anonymity, confidentiality, and triangulation were used to address the problem. Fifth, the malware threats are rapidly changing; data collected from April to May 2025 cannot necessarily reflect the future threat landscapes.

The audit focused on configurations and logs review and did not include penetration testing and zero-day simulation. Therefore, the capability of detection of unknown threats could not be verified directly. There might be selection bias since interviewed staff and audited systems may not be representative of the total population. The resource limitations and limited cybersecurity expertise may affect the availability of staff and quality of documentation. The changes in the cybersecurity policies and institutional arrangements may further impact the current relevance of the findings.

Despite these limitations, triangulation, structured sampling, validated instruments, and open reporting contributed to the credibility and relevance of the findings in relation to cybersecurity of Kenyan county governments.

Data Analysis

Quantitative Analysis: The survey data were coded and analysed in SPSS version 27. Descriptive statistics including frequencies, percentages, means, and standard deviations were used for summarizing the characteristics of respondents, self-rated malware knowledge, frequency of encounters, types of malware and infection sources. As this article addresses the first objective, namely the descriptive analysis, the inferential regression results from the parent study are not reported.

Qualitative Analysis: The interview transcripts were analysed qualitatively using thematic analysis by using the six phases outlined by Braun and Clarke (2006): familiarization, initial coding, searching for themes, reviewing themes, defining themes, and reporting. Both deductive and inductive coding were applied. Two researchers independently coded a subset of transcripts and reconciled discrepancies.

Technical Audit Analysis: The audit data were recorded using the checklist and analysed using frequencies, percentages, and means. The detection rates were calculated based on system logs when denominator data were available; however, the limitations were noted when the denominator data were not available.

RESULTS AND FINDINGS

Response Rate and Representativeness

A response rate of 90.7 percent (Table 4.1) exceeds the 70 percent which is viewed as being very good in social science studies (Mugenda & Mugenda, 2012). This high response rate is a result of continued follow-up, visits to the departments, and confidentiality promises. Each stratum in the departments had a response rate of at least 85%.

Table 4.1: Questionnaire Distribution and Return Rate

Department/Stratum	Distributed	Returned	Response Rate (%)
ICT Personnel	20	18	90.00%

Administrative Employees	35	32	91.40%
Finance Staff	30	28	93.30%
Health Records Staff	25	23	92.00%
Agricultural Staff	20	17	85.00%
Other Departments	20	18	90.00%
Total	150	136	90.70%

Data Quality

The quality of the data collected was improved by conducting pre-tests with 15 respondents, cognitive interviews, standardized delivery of the questionnaire, and data quality checks. The percentage of missing values was below 2 percent and they were sorted out during data cleaning process. Survey data was cross-validated with interview and audit results.

Distribution of Respondents by Length of Service

Table 4.2: Length of Service in Current Position

Duration of Service	**Frequency (n)**	**Percentage (%)**
Less than 1 year	18	13.2 %
1–3 years	34	25.0 %
4–6 years	52	38.2 %
More than 6 years	32	23.5 %
Total	**136**	**100 %**

Distribution of Respondents by Department

Table 4.3: Respondents by Department

Department	**Frequency (n)**	**Percentage (%)**
ICT Department	18	13.2 %
Administrative Department	32	23.5 %
Finance Department	28	20.6 %
Health (Records) Department	23	16.9 %
Agricultural Department	17	12.5 %
Other Departments	18	13.2 %
Total	**136**	**100 %**

Distribution of Respondents by Length of Service

As depicted in Table 4.2, 61.7% of the respondents were in service for more than four years; 38.2% having been in service between 4–6 years while 23.5% for more than six years. Only 13.2% of the respondents had been in service for less than one year, implying that most respondents had much knowledge about ICT security in the county.

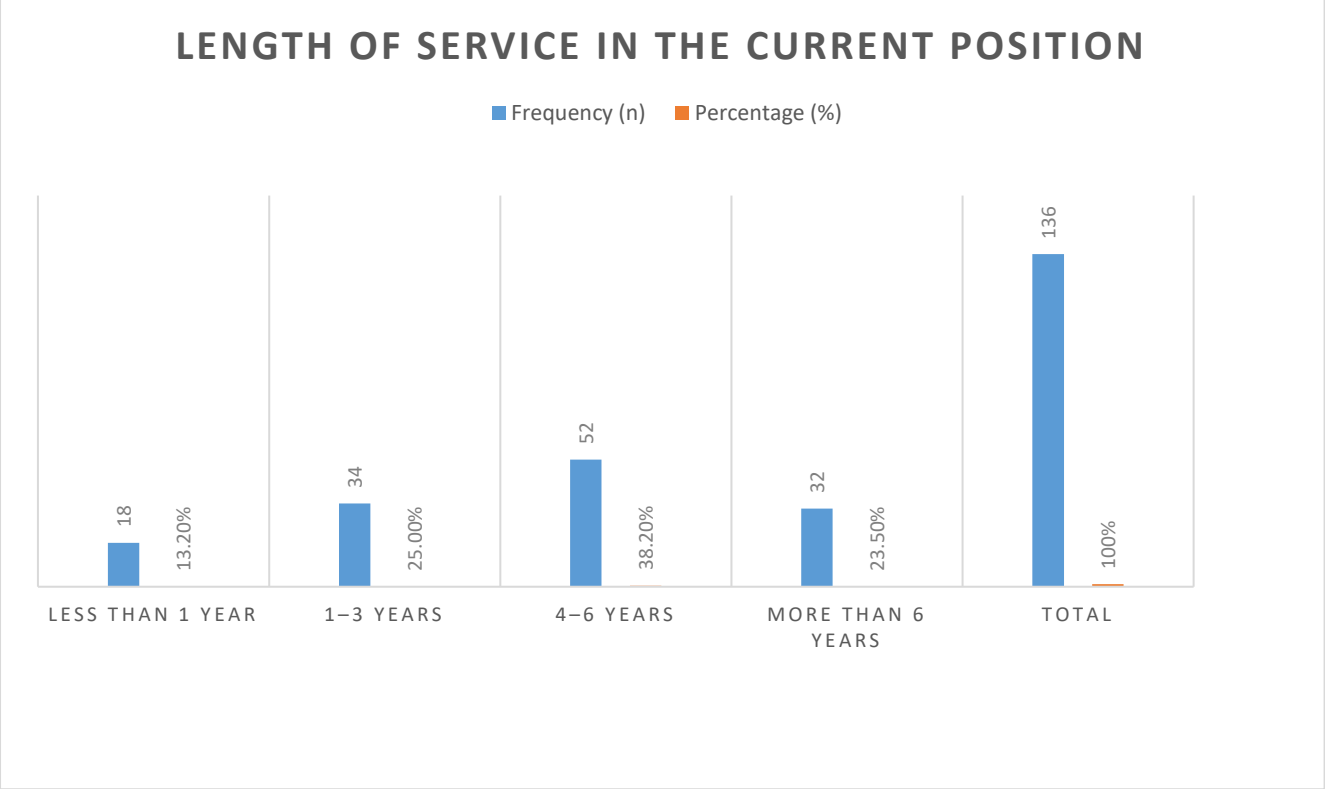

Chart 4.1: Self-Rated Knowledge of Malware Threats

Distribution of Respondents by Department

Table 4.4 shows that Administration accounted for 23.5% and Finance 20.6%. They are followed by Health Records 16.9%, ICT 13.2%, Other Departments 13.2% and Agriculture 12.5%. Technical and non-technical users participated.

Department	**Frequency (n)**	**Percentage (%)**
ICT Department	18	13.20%
Administrative Department	32	23.50%
Finance Department	28	20.60%
Health (Records) Department	23	16.90%
Agricultural Department	17	12.50%
Other Departments	18	13.20%
Total	**136**	**100%**

Current State of Malware Threats: Survey Results

Self-rated Knowledge of Malware Threats

The weighted average score on knowledge was 3.44 out of 5. Overall, 82.4% rate their knowledge as medium, high and very high while 17.7% rate their knowledge as low and very low. Nevertheless, technical audits revealed repetitive infections showing that self-perception of knowledge does not equate to being cautious. Respondents rated their knowledge of malware on a five-point scale, from 1 (very low) to 5 (very high).

Table 4.5: Self-Rated Knowledge of Malware Threats

Scale Value	Knowledge Level	Frequency (n)	Percentage (%)
5	Very high	22	16.2 %
4	High	48	35.3 %
3	Moderate	42	30.9 %
2	Low	16	11.8 %
1	Very low	8	5.9 %
Total		**136**	**100 %**

Frequency of Meeting Malware Threats

According to Table 4.5, 35.3% of respondents meet malware occasionally, while 38.3% meet malware frequently and constantly. Only 7.4% never met malware, indicating malware as a confirmed threat in the County.

Table 4.6: Frequency of Encountering Malware Threats

Level of Occurrence	Frequency (n)	Percentage (%)
Never	10	7.4 %
Rarely (less than once per year)	26	19.1 %
Occasionally	48	35.3 %
Frequently	36	26.5 %
Constantly	16	11.8 %
Total	**136**	**100 %**

Types of Malware Threats

Viruses were the most common (82.4%), followed by worms (72.1%). Third were Trojans (61.8%), then Phishing related threats (55.9%). Also, spyware (45.6%) and ransomware (27.9%) were mentioned as malware threats. Key informants emphasized phishing emails as well as potential ransomware as major threats.
Table 4.6: Types of Malware Encountered (Multiple Responses Permitted)

Malware Type	Frequency (n)	Percentage of Respondents (%)
Viruses	112	82.4 %
Worms	98	72.1 %
Trojans	84	61.8 %
Phishing-related	76	55.9 %
Spyware	62	45.6 %
Ransomware	38	27.9 %
Adware	34	25.0 %
Others	12	8.8 %

Sources of Malware Infections

Email attachments and links were the most commonly reported (76.5%). Others include removable storage (63.2%) and internet browsing (52.9%).

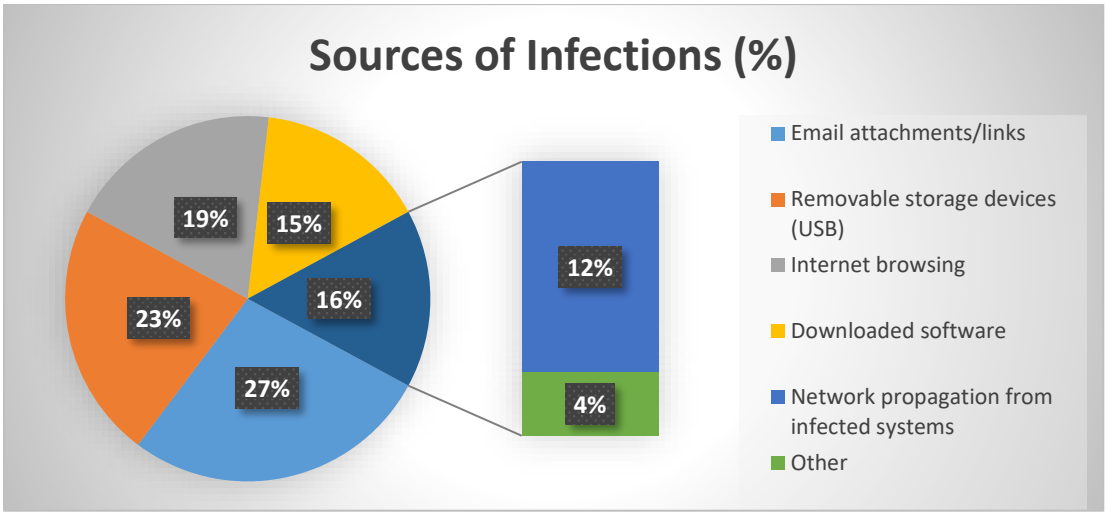

Chart 4.2 Sources of Malware Infections

Key Informant Interview Results

Four ICT key informants found two main themes: consistent underreported malware threats and risky user behaviour. Most incidents are unreported when anti-malware silently removes infection. Key informants indicated that some employees disable real-time protection features as well as click on malicious links. Therefore, the need for continuous security awareness training exists.

Technical Audit Results

The technical audit of 12 computers showed 24 malware incidents in six months of which 83.3% were handled by the anti-malware software. Four malware needed manual handling. Two recurring infections were from the same phishing source. For twelve months there were 42 detections in total including three (7%) zero-day threats. Most of the logs contain recognized malware.

Table 4.7: System Logs Audit Results (6-Month Period)

Metric	Finding
Logs available for the past 6 months	12 of 12 systems

Total malware incidents detected	24 incidents (an average of 2 per system)
Incidents resolved automatically	20 incidents (83.3%)
Incidents requiring manual intervention	4 incidents (16.7%)
False positives reported	Occasional (3 incidents)
Repeated infections from the same source	Yes (2 cases from phishing e-mails)

Results Summary

All types of results confirm malware persistence, diversity and human-related vulnerabilities. Table 4.8: Summary of Key Findings on the Current State of Malware Threats

Source	**Key Finding**
Survey	38.3% of staff encounter malware frequently or constantly; only 7.4% never do
Survey	Viruses (82.4%), worms (72.1%) and Trojans (61.8%) are the most common types; ransomware was reported by 27.9%
Survey	E-mail (76.5%) and USB devices (63.2%) are the main perceived infection vectors
Interviews	Many incidents go unreported because they are cleaned silently; user behaviour is the critical vulnerability
Technical audit	24 incidents on 12 systems in six months; two repeated phishing infections; 42 detections in twelve months, of which 3 were zero-day

CONCLUSION

Malware is a regular threat in the Homa Bay County Government which enters the system through email and removable storage devices. It is an underreported threat since infections can be silently removed. Logs reflect mostly recognized malware and do not reveal any missed threat. The results are presented in Chapter Five in relation to literature.

DISCUSSION

Interpretation of the Main Findings

Prevalence and Variety of Malware Threats

According to the responses of the participants, 38.3% of people often or persistently face malware. Viruses (82.4%), worms (72.1%), Trojans (61.8%), email attachments (76.5%), and USB devices (63.2%) are the main types of malware that constitute a threat to the Homa Bay County Government. These findings confirm the findings of the Communications Authority of Kenya (2024), Al-Duwairi and Al-Eroud (2021), Hadlington (2021), and Nobles (2022). According to the PMT, a high prevalence of threat signals is indicative of perceived severity and vulnerability; however, adequate protection requires high self-efficacy and response efficacy (Ifinedo, 2012).

Under-Reporting of Incidents

According to the key informants' responses, infections that are automatically solved do not attract attention and are not reported at all. It is possible that management understates the nature of the problem and allocates

inadequate resources for solving cybersecurity issues. Such a finding expands the literature as it stresses the need for documenting the incidents that are silently solved.

Comparison with Related Literature

The findings corroborate the world-wide, African and Kenyan literature regarding the fact that traditional malware operates side by side with advanced malware targeting governmental systems (Al-Duwairi & Al-Eroud, 2021; Ahmad & Khan, 2021; Chukwuma, 2022; Wanjiku, 2023). Compared to the previous research carried out at the county level, this study adds the perception of employees to the triangulated interview data and system logs. Altogether, this information suggests that threats might be under-assessed due to the fact that incidents are solved without being detected and due to the inability of signature-based software to detect zero-day threats.

Explanation of Unexpected Findings

While only 27.9% of respondents reported facing ransomware, ICT staff identified ransomware as their main fear, considering its potential impact compared to more prevalent malware. The finding is consistent with PMT's differentiation between the threat and the vulnerability. Furthermore, 24 incidents out of 12 systems contrasted with relatively rare reports of infections indicate automatic resolving and under-reporting. Also, the mean self-rated knowledge score of 3.44, along with frequent infections from phishing, demonstrate that knowledge does not always guarantee safe behaviour.

Implications of the Findings

Theoretical implications: The results provide empirical confirmation to PMT's differentiation between threat and coping appraisals, GDT's focus on security policy and reporting requirements, and TAM applicability to users' perceptions of protective technology.

Practical implications: The County should conduct continuous phishing-awareness training, encourage employees to use USBs safely, introduce mandatory incident reporting, document automatically solved incidents and back up offline while developing solutions for ransomware recovery.

Policy implications: At the County level, incident reporting mechanism and removable media policies should be addressed. At the National level, threat intelligence exchange between the Communications Authority of Kenya, the national Computer Incident Response Team and county governments should be improved.

Future Research: Comparative multi-county studies, longitudinal analysis of the incident logs and phishing simulation can help better understand the patterns of threat occurrence and evaluate the effectiveness of training.

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Summary of the Study The study examined the current state of malware threats faced by Homa Bay County Government. A mixed methods case study design was adopted with a structured questionnaire (136 respondents, 90.7% response rate), semi-structured interviews with four ICT key informants and technical audit of 12 systems. Questionnaire data were analysed descriptively; interview and audit data thematically and descriptively.

Summary of Key Findings

Results of the study showed that threats from malware were a daily and critical burden of risk for the county to service provision, data quality and operation (services are impacted in terms of service delivery, data integrity and business continuity). Prevalence and Frequency: The study found that malware encounters are standard not rare. 38.3% of participants reported they had been exposed to malware frequently (26.5% of study) or constantly (11.8% of all users experienced frequent (26.5%) or constant (11.8%), whereas 35.3% encountered as rare (1-2 times per year). Only 7.4% never faced malware threats. These numbers were

confirmed by technical audit results which described 24 malware incidents on 12 audited systems during a six-month period averaging 2 incidents per system in audit data.

This incidence rate is consistent with national statistics reported by the Communications Authority of Kenya (2024) which said county governments are targeted over 400,000 times a year for malware attacks. Malwares involved: The study identified various types of malwares that impact county systems. Viruses were most common among us (82.4% of respondents), worms (72.1%), Trojans (61.8%) and phishing campaigns (55.9%). Spyware was reported by 45.6% of respondents while ransomware (frequency at survey rate = 27.9%) even though it was not the most common threat cited by IT personnel as the most feared because of its potential damage was listed as the most feared threat because of its big damage potential.

The technical audit found these patterns in the log analysis too (infections were of multiple malware categories). The diversity of threats seen also means that there is a complex constantly changing threat landscape for the county and strategies for defence need to be developed with layered defence mechanism. Infection Vectors: Email attachments and links were named as main source of infection vector (76.5% of respondents). This evidence shows how human dimensions' matter to introduction of malware because phishing and social engineering attacks target behaviour not technical weaknesses.

USB drives (Removable storage devices) were second most common vectors (63.2%) and typical of the work scenario in governmental because data are often exchanged between devices. Internet browsing (52.9%) and downloads of software (42.6%) were other major sources. These results show that technical controls alone aren't enough — awareness of the user and behaviour modification are as important as technical controls to have an effective defence strategy.

User Knowledge and Awareness: Even though 82.4% feel they know malware threats somewhat moderate to high, technical audit was missing information from understanding about security measures (e.g.: even though self-assessed knowledge there were cases of "re-infections" from the same attack vector e.g., phishing email). So knowledge is not always reflected in safe behavioural behaviour. This result confirms Protection Motivation Theory which states that threat appraisal (awareness level of the threat) has to be associated with coping appraisal (confidence in one's ability to react effectively to that threat) in order for protective behaviours to motivate.

Underreporting of incidents: Qualitative data from key informant interviews showed a great many malware incidents are not being reported — low-level trivial infections that anti-malware programs automatically clean up (staff don't report them unless their PC comes down or they see something like a pop-up', said one system administrator). Many infections can be silently cleaned away by anti-malware software and the user never even knows it." This underreporting gives people a false sense of security and hides the true threat scale so resources and attention may be underestimated.

Conclusions

Homa Bay County Government are under wide spread and ongoing threat of malware. Surveys, interviews and technical audits show exposure to malware is common not unusual (evidence builds credibility over time), the types of malware (ordinary viruses & worms to complex Trojans & phishing) show that threats are large and changing and human factors (email and USB devices) are entry points for primary infection vector so that technical controls can reduce risk but awareness campaigns need to address both.

Conclusion 2: Malware incidents are very poorly reported. Because they are automated many infections can be automatically resolved without user knowledge (common false assurance that infection severity is quite low), hiding the real threat scale. Underreporting can cause management to think the need is also being recognized — and so under-invest in cybersecurity continues.

Conclusion 3: User knowledge does not equal secure behaviour. However, even though perceived knowledge of malware threats was relatively high, technical audit showed multiple infections from the same sources and

weak configurations (e.g. repeated infections from the same phishing source) so awareness vs practice gap exists. Therefore awareness programs will need to go beyond knowledge dissemination and also behaviour modification/training.

Recommendations. The recommendations below follow from the findings and are addressed to the actors who can act on them.

Recommendations for Homa Bay County Government i. Run continuous phishing focused awareness training. E-mail is the main infection vector and repeated phishing infections were found so training should be repeated role specific and supported by regular simulated phishing exercises with results used to target staff who need further support.

Control removable media: the County should have a policy on use of USB devices, scan all removable media automatically and restrict or disable unmanaged devices on sensitive systems (Finance and Health Records departments). Create a simple mandatory incident reporting channel. Staff should be able to report suspicious messages and system behaviour in one step, ICT Department should record and report silently resolved incidents to management so that the real scale of threat is visible.

Centralise logging and monitoring: logs from all systems should be collected and reviewed in one place (at least monthly) so patterns like repeated infections from the same source can be detected early on. Managed or cloud based monitoring service may reduce upfront cost. Prepare for ransomware. The County should have offline backups of critical systems and data; test restoration regularly; update incident response plan (last reviewed ten months before audit) to include ransomware scenario.

Recommendations for National Government and Regulators. The Ministry of ICT and Communications Authority of Kenya should share timely threat intelligence with county governments, provide a simple channel for counties to report malware incidents and include indicators at the county level (share of staff that encounter malware; number of incidents recorded) in monitoring of the National Cybersecurity Strategy 2022–2027.

Limitations of the Study. The study was a single case study of Homa Bay County Government so findings cannot be statistically generalized to other counties but pattern of threats is consistent with national literature; survey relied on self-reported experience which has recall and social desirability bias; technical audit was on a purposively selected sample of 12 systems over a limited period; cross sectional design captures threat environment at one point in time; audit logs show only threats that installed tools were able to detect.

Recommendations for Further Research.

- Multi-county studies to compare threat profiles and identify variation across counties.
- Longitudinal studies of incident logs to track the evolution of the threat environment.
- Phishing-simulation and experimental studies to test the effect of different training approaches on actual user behaviour.
- Studies of incident under-reporting in the public sector (organizational reasons why incidents are not reported).

Contribution to Theory and Practice. Theoretically it combines PMT, GDT and TAM jointly to describe a malware threat environment (and shows that awareness of threat does not lead to protective behaviour); practically it describes the threats faced by a county government baseline; entry points and reporting gaps on which limited resources should be concentrated; methodologically how survey perceptions, interview evidence and system logs can be triangulated to produce a more reliable description of exposure to threats.

Final Conclusion. Homa Bay County Government works in an environment where malware is a daily occurrence and in which the main entry points are the actions staff take on a daily basis. The exposure of the County will be much greater than the reported figures suggest. In the first place the most effective response is to strengthen user behaviour, reporting and monitoring (which can be done with very little resources) while the County builds the stronger technical defences described in companion manuscripts

REFERENCE

1. Adeyemi, O. (2022). Anti-malware strategies in African public sector organizations. African Journal of Information Security, 12(1), 35-50.
2. African Union. (2023). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention): Status of ratification. African Union.
3. Ahmad, M., & Khan, A. (2021). A comprehensive study on global malware threats and mitigation strategies. Journal of Cyber Security, 15(3), 102–117.
4. Al-Duwairi, B., & Al-Eroud, A. (2021). Current trends and future directions in malware analysis and detection. Journal of Information Security and Applications, 58, Article 102827.
5. Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. Journal of the Association for Information Systems, 8(4), 244–254.
6. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. MIS Quarterly, 39(4), 837–864.
7. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
8. Chukwuma, E. (2022). Cybersecurity challenges in African government institutions: A focus on malware. African Journal of Information Security, 10(2), 45–60.
9. Communications Authority of Kenya. (2024). Annual cybersecurity report 2023/2024. Communications Authority of Kenya.
10. Creswell, J. W., & Creswell, J. D. (2021). Research design: Qualitative, quantitative, and mixed methods approach (5th ed.). SAGE Publications.
11. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.
12. D'Arcy, J., Hovan, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98.
13. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
14. De Leeuw, E. D. (2018). Mixed-mode: Past, present, and future. Survey Research Methods, 12(2), 75–89.
15. Denzin, N. K. (1978). The research act: A theoretical introduction to sociological methods (2nd ed.). McGraw-Hill.
16. DeVellis, R. F., & Thorpe, C. T. (2021). Scale development: Theory and applications (5th ed.). SAGE Publications.
17. Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Behavior Research Methods, 41(4), 1149–1160.
18. Fefferman, N. H., & Sverchkov, M. (2025). Addressing selection bias in nonprobability samples: Methodological considerations for mixed-methods research. Journal of Survey Statistics and Methodology, 13(1), 45–68.
19. Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). SAGE Publications.
20. Fowler, F. J. (2014). Survey research methods (5th ed.). SAGE Publications.
21. Gibbs, J. P. (1975). Crime, punishment, and deterrence. Elsevier.
22. Green, S. B. (1991). How many subjects does it take to do a regression analysis? Multivariate Behavioral Research, 26(3), 499–510.
23. Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. Plops ONE, 15(5), Article e0232076.

24. Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. In P. B. Lowry, J. D'Arcy, & B. Hammer (Eds.), Human aspects of information security and assurance (pp. 45–62).
25. Hair, J. F., Page, M., & Brunsveld, N. (2021). Essentials of business research methods (4th ed.). Routledge.
26. Hardesty, D. M., & Bearden, W. O. (2004). The use of expert judges in scale development: Implications for improving face validity of measures of unobservable constructs. Journal of Business Research, 57(2), 98–107.
27. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106–125.
28. Homa Bay County Government. (2024). County integrated development plan 2023-2027. Homa Bay County Government.
29. Homa Bay County ICT Department. (2024). Annual ICT security incident report January 2023-June 2024. Homa Bay County Government.
30. Homa Bay County Treasury. (2024). County budget implementation review report 2023/2024. Homa Bay County Government.
31. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. Computers & Security, 31(1), 83–95.
32. International Telecommunication Union. (2023). Global Cybersecurity Index 2023. International Telecommunication Union.
33. Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: A guide to conducting a semi-structured interview study. Scandinavian Journal of Caring Sciences, 30(2), 295–304. Kaspersky Lab. (2024). Malware taxonomy and classification: Annual threat report. Kaspersky Lab.
34. Kenya. (2018). Computer Misuse and Cybercrimes Act, No. 5 of 2018. Government Printer.
35. Kenya. (2019). Data Protection Act, No. 24 of 2019. Government Printer.
36. Kenya National Audit Office. (2023). Report of the Auditor-General on the ICT systems security in county governments. Kenya National Audit Office.
37. Kenya National Bureau of Statistics. (2022). Kenya population and housing census: County statistical abstract - Homa Bay.
38. Kenya. (2022). National Cybersecurity Strategy 2022-2027. Ministry of ICT, Innovation and Youth Affairs. Ministry of ICT, Innovation and Youth Affairs.
39. Kshetri, N., & Voas, J. (2023). Ransomware attacks on critical infrastructure: Patterns and implications. IEEE Computer, 56(3), 56-64.
40. Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.
41. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469–479.
42. Merriam, S. B., & Tisdell, E. J. (2016). Qualitative research: A guide to design and implementation (4th ed.).
43. Ministry of ICT, Innovation and Youth Affairs. (2023). Digital Economy Blueprint: Transforming Kenya through digital innovation. Government of Kenya.
44. Mugenda, O. M., & Mugenda, A. G. (2012). Research methods: Quantitative and qualitative approaches (3rd ed.). African Centre for Technology Studies Press.
45. National Institute of Standards and Technology. (2020). Guide to malware incident prevention and handling for desktops and laptops (NIST Special Publication 800-83 Revision 1). National Institute of Standards and Technology.
46. Ng, B. Y., & Rahim, M. A. (2005). A socio-behavioural study of home computer users' intention to practice security. Proceedings of the Ninth Pacific Asia Conference on Information Systems, 1234-1245.
47. Njenga, M. (2023). Effectiveness of anti-malware systems in Kenyan county governments: A case study of Kisumu County. Kenya Journal of Information Systems, 6(1), 102-118.
48. Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity professionals: A human factors perspective. Computers & Security, 115, Article 102612.
49. Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

50. Odhiambo, P., & Mwangi, S. (2023). Challenges in implementing ICT security measures in Kenyan county governments. East African Journal of Information Science, 7(2), 112- 128.
51. Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533–544.
52. Patel, K., & Soni, D. (2022). Evaluation of modern anti-malware solutions in organizational settings. Cybersecurity, 5(1), Article 19. Patton, M. Q. Qualitative research and evaluation methods (4th ed.). SAGE Publications.
53. Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems, 32(4), 179-214.
54. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.
55. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153-176). Guilford Press.
56. Ryan, M. (2025). Mixed-methods approaches to organizational incident response research: Lessons from cybersecurity case studies. Journal of Mixed Methods Research, 19(2), 156–178.
57. Savenko, O., Lysenko, S., & Kryshchuk, A. (2022). Metamorphic malware detection using machine learning techniques: A comprehensive review. Journal of Computer Virology and Hacking Techniques, 18(3), 201-222.
58. Serianu. (2023). Africa cybersecurity report: Kenya country report. Serianu Limited.
59. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.
60. Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. Research in Science Education, 48(6), 1273–1296.
61. Taherdoost, H. (2022). Sampling methods in research methodology: How to choose a sampling technique for research. International Journal of Academic Research in Management, 11(1), 18-27.
62. Thompson, S. K. (2012). Sampling (3rd ed.). John Wiley & Sons.
63. United Nations. (2023). Report of the Secretary-General on developments in the field of information and telecommunications in the context of international security. United Nations General Assembly.
64. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204.
65. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.
66. Wanjiku, M. (2023). Malware threats and cybersecurity measures in Kenyan county governments. Kenya Journal of Information Systems, 5(1), 78-92.
67. World Economic Forum. (2024). The Global Risks Report 2024 (19th ed.). World Economic Forum.
68. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.