Effectiveness of Anti-Malware Security Technologies in Homa Bay County Government, Kenya.

Okura Odhiambo James

Great Lakes University Kisumu

DOI: https://doi.org/10.47772/IJRISS.2026.101000646

Received: 19 October 2026; Accepted: 24 October 2026; Published: 13 November 2026

ABSTRACT

County governments in Kenya depend on information systems for public service delivery and invest in anti-malware technologies to protect sensitive information but effectiveness of these technologies is rarely evaluated. The second of three articles from the author's MBA research evaluated anti-malware security technologies deployed by Homa Bay County Government. Effectiveness was operationalised as detection, prevention, incident frequency, response time, update and patching practices, user awareness and perceived effectiveness. Convergent mixed methods case study design was used. Data were collected in April–May 2025 through a structured questionnaire (150 distributed; 136 returned; 90.7%), semi-structured interviews with four ICT key informants and technical audit of 12 systems (2 servers; 10 workstations). Questionnaire data were analysed descriptively using descriptive statistics and multiple linear regression, interviews thematically and audit data descriptively. Anti-malware software was installed on all 12 audited systems and reported by 85.3% of respondents (Windows Defender for Endpoint (62.1%) and Kaspersky Endpoint Security (41.4%) were most often mentioned by those with software installed). Real time protection was enabled on all audited systems; automatic updates and cloud threat intelligence were enabled on 83.3%; heuristic detection was enabled on 75%; scheduled scans on 66%; operating systems updated fully on 83.3% and third party applications on 66%. Internal logs showed a detection rate of 95% compared to 88% in independent scans and average response time was two hours. Three of 42 detections (7.1%) were zero-day threats (without a controlled zero-day test this suggests but does not prove limited detection of unknown malware); perceptions were more positive than audit evidence. Effectiveness was rated moderate or high by 82.4% of respondents (57.4% satisfied) but perceptions were higher than evidence from the audit. The regression model explained 61.2% of variance in perceived effectiveness ($R^2 = 0.612$; $F(6, 129) = 33.94$; $p < 0.001$); staff training ($\beta = 0.356$) and patch management ($\beta = 0.312$) were the strongest predictors followed by user awareness, resource allocation and technology type and policy enforcement was not significant. The technologies provide a baseline protection against known threats but are moderately effective because configuration gaps exist, patching is inconsistent, products are fragmented and little evidence that emerging threats are detected. A phased programme is recommended: first correct configuration and patching within existing licences and budgets then standardise and centralise platform and add behaviour based detection and server protection as funds allow.

Keywords: Anti-Malware Effectiveness; Endpoint Protection; Signature Based Detection; Patch Management; Technical Audit; County Government; Kenya.

INTRODUCTION

Background to the Study Malware refers to malicious software designed to harm computer systems, servers, clients or networks. It includes various types, such as viruses, worms, Trojan horses, ransomware, spyware, adware and file-less malware. These threats exploit vulnerabilities of information systems to access sensitive information, disrupt information system operation, steal information, extort ransoms or create unauthorised access for future attacks (Kaspersky Lab, 2024). Malware of modern days uses polymorphism, metamorphism and encryption to evade traditional signature-based detection (Savenko et al., 2022).

Cyberattacks represent one of the major threats to information systems and critical infrastructure of government entities in different parts of the world. According to the World Economic Forum (2024), cyberattacks represent one of the major global risks, whereas according to International Telecommunication Union (2023), there are continued gaps in cybersecurity implementation despite the adoption of national cybersecurity strategies by many countries. Examples of such cyberattacks include Colonial Pipeline ransomware, WannaCry against the UK's National Health Service, and NotPetya against Ukrainian government systems (Kshetri & Voas, 2023).

In Africa, rapid development of Internet access and digital transformation provide opportunities for socio-economic development, yet increase the exposure to cyber threats. Africa Cybersecurity Report (2023) indicates that malware represents one of the contributors to successful cyberattacks on African governments, while Interpol (2024) identifies ransomware, banking Trojans and business email compromise as cyber threats faced by African governments. Limited technical expertise, cybersecurity budget and weaknesses in cyber defences add to cybersecurity challenges.

Kenya is developing new digital transformation initiatives, such as e-Citizen and Huduma Kenya, which increases the reliance on information systems and amount of sensitive information stored electronically. In particular, the Communications Authority of Kenya (2024) reported about cyber threat activity increase during the 2023/2024 financial year including malware attacks. However, in the context of decentralised ICT infrastructure, sufficient cybersecurity budget and capability are not always allocated.
Homa Bay County Government delivers public services in eight sub-counties in several sectors including health, finance, education, agriculture and ICT. These services rely on information systems holding sensitive patient, financial, personnel and administrative information. Thus, any malwares incidents can affect the continuity of services, confidentiality of information and public confidence.

Effective anti-malware systems are not only about installation, but also about their ability to detect threats, prevent malicious execution, enable timely response, keep the software up-to-date and perform consistently. Various factors at organisational level, such as staff competence, cybersecurity awareness, patch management, enforcement of policies and resources availability, influence the performance of the technologies

The current study is informed by Protection Motivation Theory (PMT), General Deterrence Theory (GDT) and Technology Acceptance Model (TAM). These theories explain how the interaction of individual behaviour, organisational controls and acceptance of technologies affect cybersecurity outcomes. The previous studies indicate signature-based detection, outdated technologies, and insufficient user awareness as major recurring challenges (Al-Duwairi & Al-Eroud, 2021; Chukwuma, 2022; Wanjiku, 2023).

Even with increased awareness of the importance of cybersecurity, the recent studies related to county government do not provide evidence on the performance of anti-malware technologies. This study evaluates the effectiveness of anti-malware technologies implemented in Homa Bay County Government, which will serve as a basis for better cybersecurity practices in devolved government institutions.

Problem Statement

County governments in Kenya experience malware attacks even in the presence of anti-malware technologies. This situation raises the question about whether such systems can detect, prevent and mitigate malware attacks. In Homa Bay County Government, incidents reported include ransomware which affects access to health records, spyware that compromises personnel information and Trojan attacks affecting financial transaction systems (Homa Bay County ICT Department, 2024).

The background of the current study includes the report of 147 documented malwares cases occurring between January 2023 and June 2024. Also, there are mentioned configuration gaps, inconsistent patching and dependence on signature-based detection. Such configuration problems can lead to such consequences as system downtime, data corruption, unauthorized access and disruption of public services. Such incidents may result in delayed salary payments, interference with patient management and restriction of access to

agricultural information. Besides, they can result in costs for county government and decrease in public trust to government ability to protect personal information.

While the international studies examined malware detection technologies, and the African studies explored challenges in public sector cybersecurity, there is scarce evidence on the effectiveness of anti-malware systems in Homa Bay County Government. The previous studies in Kenya mainly focused on malware prevalence or another county without technical assessment of the performance of deployed technologies. In terms of methodology, most studies use either employee perceptions or technical test, but not both approaches. As a consequence, favourable perceptions do not necessarily reflect the performance of systems.
This journal tries to answer the following specific question: whether anti-malware technologies deployed in Homa Bay County Government detect, prevent and mitigate malware attacks.

This journal answers four questions: which anti-malware technologies Homa Bay County Government has deployed and how they are configured; how well they detect and prevent malware, limit incidents, support timely response and keep systems up to date; how employees' perceptions compare with technical evidence; and which factors are associated with perceived effectiveness.

Study Justification

Increasing reliance of county governments on information systems for service delivery raises cybersecurity risks. Although anti-malware technologies are widely deployed, the frequent attacks raise the question about their effectiveness and adequacy of cybersecurity investments.
International priorities, such as creation of secure digital infrastructure under Sustainable Development Goals 9 and 16, make necessary to implement resilient information systems and efficient governance. Regionally, the African Union Convention on Cyber Security and Personal Data Protection creates a basis for improved cybersecurity and protection of personal information.

In Kenya, the Digital Economy Blueprint and National Cybersecurity Strategy 2022-2027 stress secure digital transformation. Nevertheless, evidence on the effectiveness of anti-malware systems in devolved government institutions remains scarce. Homa Bay County Government serves as a suitable location for exploring how technical controls, human and organizational factors interplay in the context of resource-constrained public sector. This study is justified by the need to establish whether deployed technologies adequately protect county information assets. Comparing perceptions of employees with technical audit results and identifying the factors contributing to the effectiveness will help to fix configuration issues, choose new product, train employees and allocate resources.

1.4.1 Main objective. To assess the effectiveness of anti-malware security technologies in Homa Bay County Government.

1.4.2 Specific objectives

1. to identify the anti-malware products used and how they are configured;
2. technical effectiveness (detection, prevention, incident frequency response time update and patching practices);
3. compare employees' perceived effectiveness with technical audit evidence;
4. relationship between staff training patch management technology type user awareness policy enforcement resource allocation and perceived effectiveness.

Research Questions

RQ1: What anti-malware products are deployed in Homa Bay County Government and how are they configured?

RQ2: How effective are they (detection, prevention, incident frequency, response time etc.) update and patching practices)?

RQ3: How do employees' perceptions of effectiveness compare with the technical audit evidence?

RQ4: Which factors are associated with perceived effectiveness?

Hypotheses (RQ4, $\alpha = 0.05$).
H1–H6: staff training, patch management, technology type, user awareness, policy enforcement and resource allocation are each positively and significantly associated with perceived effectiveness (null hypothesis in each case is no association).

Objective	Research question	Key indicators	Data source and analysis	Results	Conclusion
1. Products and configuration	RQ1	Products in use; real-time protection, auto-update, heuristic, cloud and scheduled-scan settings	Questionnaire (descriptive); audit checklist	4.3 – 4.4	6.4 First, Third
2. Technical effectiveness	RQ2	Detection, prevention, incident frequency, response time, update and patching	Audit logs, console data, independent scan, vulnerability scan (descriptive); interviews (thematic)	4.5, 4.9, 4.10	6.4 First, Second, Fourth
3. Perception against audit	RQ3	Perceived effectiveness and satisfaction against Objective 2 indicators	Questionnaire compared with audit (Table 4.14)	4.6 – 4.7	6.4 Sixth (new)
4. Associated factors	RQ4, H1–H6	Perceived Effectiveness Index regressed on six factors	Multiple linear regression (n = 136); interviews	4.8 – 4.9	6.4 Fifth

Table 1.1. Alignment table

Significance of the Study

The current study adds evidence about the effectiveness of anti-malware technologies in Kenyan county governments combining the results of employee perceptions and technical audit. It identifies configuration weaknesses, patching gaps and organizational factors associated with effectiveness. For Homa Bay County Government, the findings will help to improve the configuration of deployed systems, choose appropriate product, train employees and allocate resources. Other counties and procurement agencies can use the audit methodology to assess their systems. The researchers will get the benefit from the empirical demonstration of the importance of comparison of perceived effectiveness with objectively measured technical performance.

Scope and Delimitation

The current study focuses on the anti-malware technologies deployed in Homa Bay County Government. It explores their installation, configuration, detection performance, update status and effectiveness using questionnaires, interviews and technical audits. The geographical scope of the study is limited to ICT systems

of Homa Bay County Government offices. Private organizations, NGOs and other county governments are excluded from the study. Firewalls, intrusion detection systems, physical security and forensic investigation of historical breaches are not assessed. This journal focuses on the effectiveness of deployed anti-malware technologies and organizational factors related to it. Malware prevalence and implementation challenges are covered in the companion journal.

Assumptions

The current study is based on the assumptions that ICT systems and anti-malware tools in Homa Bay County Government remain reasonably stable during data collection, the respondents provide valid information, the chosen employees and systems represent the study environment and relevant technical logs, configurations and incident reports are available.

Definition of Key Terms

Cybersecurity: measures used to protect computer systems, networks and information from unauthorised access, misuse or damage.

Malware: software intentionally created to harm, exploit or gain unauthorized access to information systems.
Anti-malware systems: software and technologies used to detect, prevent and remove malicious software.

Effectiveness: how well deployed anti-malware technologies detect malware, prevent infection, reduce incident frequency, enable timely response, stay up to date and are perceived by users to protect them. It is measured with seven indicators (Table 3.2): detection, prevention, incident frequency, response time, update and patching practices, awareness and perceived effectiveness. Technical indicators come from the audit; user awareness and perceived effectiveness come from questionnaire.

Signature-based detection: identification of malware via comparison with known malware signatures.

Heuristic or behaviour-based detection: identification of potential threats based on file characteristics and suspicious behaviour without the need for the signature alone.

Zero-day threat: previously unknown threat for which there is no signature or patch available yet.
Patch management: process of identification, testing and application of software patches to correct vulnerabilities.

Mixed-methods approach: a research design that uses quantitative and qualitative evidence to provide a comprehensive understanding of a research problem.

LITERATURE REVIEW

Theoretical Framework

The current study is guided by Protection Motivation Theory, General Deterrence Theory and Technology Acceptance Model. They explain individual, organizational and technological factors influencing the effectiveness of anti-malware technologies.

Protection Motivation Theory

Protection Motivation Theory, introduced by Rogers (1975), explains how people respond to the perceived threats and adopt protective behaviours. This theory considers two major processes: threat appraisal and coping appraisal.Threat appraisal deals with perceived threat severity and vulnerability. In the current study, it reflects employees' perceptions of malware threats, including information leakage, financial theft and interruption of service delivery.

Coping appraisal involves perceived ability to cope with or prevent threats. It includes response efficacy, self-efficacy and response costs. People are more willing to follow protective measures when they are convinced that the measures are effective, feel capable of implementing them and find the costs reasonable (Maddux & Rogers, 1983). PMT explains why installed anti-malware technologies underperform in the cases when employees underestimate the threats, doubt the security measures or have problems with their utilization. Training and security awareness will enhance protective behaviour and proper usage of deployed technologies. The literature (Infineon 2012; Boss et al., 2015) demonstrates the relevance of threat and coping appraisals in relation to information security compliance. Nevertheless, PMT tends to understate the role of organizational culture, social norms and habitual behaviour. Despite its weaknesses, PMT is helpful to explain individual factors related to anti-malware effectiveness.

General Deterrence Theory

General Deterrence Theory, associated with Gibbs (1975), explains how certainty, severity and swiftness of sanctions influence human behaviour. In the context of information security, employees will not engage in risky behaviour if they believe that their violations will be detected and punished the current theory is relevant for the cybersecurity policy, acceptable-use requirements, monitoring systems and disciplinary actions. Employees who understand consequences of disabling security software, using unauthorised devices and clicking malicious links are more likely to comply with security measures.

The literature (D'Arcy et al., 2009; Herath & Rao, 2009) supports the importance of awareness of security regulations, monitoring and sanctions in reducing intentions of information system abuse. Nevertheless, deterrence will be reduced in case of inadequate monitoring and inconsistent sanctions. So, GDT helps to explain organizational conditions under which the anti-malware technologies operate, although its predictive value will depend on enforcement capability.

Technology Acceptance Model

Technology Acceptance Model, developed by Davis (1989), explains the technology acceptance by means of perceived usefulness and perceived ease of use. Perceived usefulness means people's belief that technology improves their performance while perceived ease of use implies the level of effort required to use technology. Both beliefs determine acceptance and actual usage of technology. In the current study, TAM explains how county employees' perceptions of anti-malware technologies influence their willingness to use them correctly, update regularly and respond to security warnings. Those employees, who perceive the security tools as useful and easy to use, will cooperate with protective measures. At the same time, the users who see the tools as disruptive and difficult will ignore warnings, turn off some features and look for alternatives.

Training, technical support and system design can improve the perceptions. The literature (Venkatesh et al., 2003; Ng & Rahim, 2005) supports the importance of technology acceptance factors in explaining technology usage. However, TAM will be less explanatory where technology usage is obligatory. Nevertheless, it remains relevant because mandatory installation does not mean proper use and positive perceptions.

Integration of Theories and Connection to Study Variables

The three theories provide complementary explanations of anti-malware effectiveness. The principal theoretical lens in this case is TAM, which explains user acceptance and perceptions of deployed technologies. PMT explains how threat perceptions, training and self-efficacy influence the protective behaviour, while GDT explains how policies, monitoring and sanctions affect compliance.

So, all three theories recognize that effectiveness of cybersecurity depends on the interaction of technology, individuals and organizational controls. The advanced tools may underperform in case of the lack of skills, cybersecurity policy weaknesses and difficulty of the technologies usage. This means that technology type, employee training, user knowledge, patching, resource availability and policy enforcement can be assessed with respect to the effectiveness of anti-malware technologies in Homa Bay County Government

EMPIRICAL LITERATURE.

Effectiveness of Anti-Malware Security Technologies.

Effectiveness of anti-malware security technologies is measured by their ability to detect malware samples, false positives, response time, performance impact, and identification of new types of malware. Previous research proves that there is much difference in these characteristics among various technologies. Patel and Soni (2022) used 12 different products, commercial and open-source, to test their performance by using 10,000 samples, both known and zero-day. Signature-based technologies detected 92-98% of the known malware but only 23-45% of the unknown malware samples. Heuristic and machine learning-based technologies detected 62-78% of the zero-day samples, however, they had more false positives than signature-based ones. Cloud-based technologies had higher detection speed due to cloud-based threat intelligence.

It can be seen from this research that good performance against known malware does not mean good performance against unknown malware. However, this experiment can have some limitations due to the fact that laboratory testing cannot cover all conditions present in real organisational settings. Smith and Perez (2021) studied anti-malware technologies in the information systems of governments of 15 countries. It was found that signature-based technologies still dominate and only 34% of sampled organisations used behaviour-based or artificial intelligence-based technologies. Also, 67% of the sampled organisations had experienced zero-day malware attack during the last two years. Regular training of users improves their perception of the security tools used and decreases the number of workarounds, however, due to the nature of the self-reported information, it is hard to attribute success only to anti-malware tools.

In Africa, public sector organizations often used basic signature-based technologies, did not have proper updates and integration of the software. Advanced functions were turned off due to concerns about high false positive rate and impact on the performance of the systems. It shows the difference between the advertised capabilities of the technology and its actual use in practice.

In Kenya, Wanjiku (2023) found that counties, which used centralized ICT management, automatic updates, and regular audit of the systems, had detection rates, which were 35% higher than those of counties, which used decentralized approach. Counties with regular training sessions of the employees had 41% lower number of successful attacks. However, the limitations of the cross-sectional design of the study limit the conclusions about the causality. Njenga (2023) studied the effectiveness of anti-malware tools in Kisumu County. Signature-based detection detected 94% of the known malware samples but only 31% of the zero-day samples.

Only 38% of all detected threats could be solved without any manual intervention. Automatic updates were associated with 73% fewer successful attacks than manual updates. Integration of anti-malware technologies with firewalls, intrusion detection and security information and event management software was limited. It can be seen that effective anti-malware protection involves not only the purchase of the technologies but also configuration, timely updates, employee training, centralization and ability to detect unknown malware.

Summary of Empirical Literature and Identification of the Research Gap.

Author (Year)	Key Findings	Identified Research Gap
Patel & Soni (2022)	Signature-based solutions: 92–98% detection for known threats and 23–45% for zero-day; AI/heuristic solutions: 62–78% zero-day detection with 8–15% false positives; cloud integration reduced detection time by 4.7 hours.	Laboratory setting may not reflect real organizational complexity; limited examination of resource-constrained environments.
Smith & Perez (2021)	Only 34% of government organizations adopted behaviour-based or AI-driven solutions; 67% experienced zero-day infections; user training significantly improved perceived usefulness.	Self-reported data; difficulty in isolating anti-malware effectiveness from other security controls.
Adeyemi (2022)	Most African public sector organizations rely on basic signature-based tools owing to resource constraints; advanced features are often disabled for performance	Continental overview without technical verification of configuration or detection.

	reasons.	
Njenga (2023)	Signature-based detection 94% for known and 31% for zero-day threats; only 38% of threats resolved without manual intervention; automated updates correlated with 73% fewer infections.	Single-county focus limits generalizability; cross-sectional design prevents causal conclusions.

CONCEPTUAL FRAMEWORK

The conceptual framework for this paper is presented in order to highlight the variables that will affect the efficiency of anti-malware systems. The dependent variable will be efficiency of the anti-malware system which involves detection, prevention, response and recovery from attacks on the system as well as performance of the system and its users' satisfaction level. The independent variables will be anti-malware technology and its configuration, patch management, training, awareness and policy implementation.

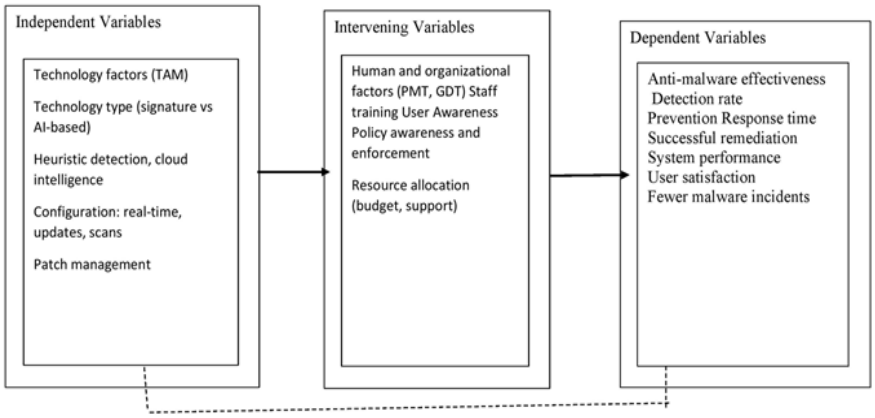


Figure 2.2: Conceptual Framework for the Effectiveness of Anti-Malware Technologies

Theoretical Anchoring

The proposed conceptual framework is anchored on the Technology Acceptance Model (Davis, 1989) that postulates the effect of usefulness and ease of use on the use and proper functioning of security tools; Protection Motivation Theory (Rogers, 1975) that explains how self-efficacy and response efficacy developed through training shape protective behaviour; and General Deterrence Theory (Gibbs, 1975) that states the effect of policies and enforcement on compliance. Therefore, the effectiveness of anti-malware tools can be seen as the result of interplay of technology, people and organisational controls

Assumptions of the Framework

The assumptions of the proposed framework are that the variables are measurable using questionnaires, interviews and technical audits; relationships among independent and dependent variables are predominantly linear; and the external variables do not change significantly. Moreover, it is assumed that the respondents are adequately informed and have good recollection abilities; the ICT infrastructure of the County and its security policies remain unchanged; the selected systems represent the typical security environment of the County; and influence flows from independent variables to anti-malware effectiveness

RESEARCH METHODOLOGY

Research Design

A mixed-methods case study design was used in the study, whereby the quantitative data was collected using questionnaires and the qualitative one using interviews and technical system audits. While the questionnaires were aimed at capturing perceptions and experiences of the employees, interviews were conducted with ICT

key informants, and the technical audit involved examining system configurations and log files. The case study approach was appropriate since the study focused on investigating the effectiveness of anti-malware tools in the context of ICT infrastructure of Homa Bay County Government (Yin, 2018). The use of triangulated survey, interview and audit evidence helped increase credibility and trustworthiness of the results (Denzin, 1978; Patton, 2015). Furthermore, it was helpful in identifying gaps between the actual and perceived performance of the system. Each instrument was designed to answer a specific research question (Table 1.1).

Research Design.

The case study approach was suitable because the study examined a bounded system within Homa Bay County Government's ICT infrastructure and personnel within its real-life context (Yin, 2018). Triangulation of survey, interview, and technical audit data enhanced the credibility of findings (Creswell & Poth, 2018).A convergent mixed-methods case study design was used (Yin, 2018; Creswell & Creswell, 2021). Quantitative data came from the questionnaire (n = 136) and technical audit of 12 systems which was analysed descriptively. Qualitative data came from semi-structured interviews with four ICT key informants and auditor's observations. The three strands were collected over the same eight weeks' period, separately analysed and merged at interpretation (Table 4.14), so perceived effectiveness could be compared with measured performance.

The inclusion of these methods in triangulation increased validity because information was triangulated. Triangulation (using several sets of sources/methods or investigators to support or confirm evidence) also increases trustworthiness of research findings (Denzin, 1978; Patton, 2015). Ryan's (2025) study on incident response of organizations showed during mixed-methods research: triangulation of survey data with in-depth interviews identifies the systematic perception gaps that may not be visible before (e.g., experience of professional communities with cybersecurity). Also a mixed-method design used in our recent study on the analysis of teaching log data in constrained-resource settings (faculty questionnaires combined with learner performance measures) showed how sequential method can capture institutional and cognitive dimensions of cybersecurity issues. Through this methodological approach we made sure that technical realities, user opinions and organizational pressures were covered and investigated throughout the study.

Study Area/Site Description

Homa Bay County is located in the western part of Kenya adjacent to Lake Victoria and has a population of approximately 1.2 million people (Kenya National Bureau of Statistics, 2022). It provides services through different departments such as administration, health, agriculture, ICT, finance, education and municipal services. The ICT Department of the County manages approximately 1,200 network devices including desktops, laptops, servers and other network peripherals in its headquarters and sub-counties. Homa Bay County was chosen due to known malware cases and the resource limitations of the devolved government entities (Homa Bay County ICT Department, 2024; Njenga, 2023).

Target Population

The target population consisted of employees who use ICT systems regularly. There were two categories of the population. Firstly, there were 28 technical ICT staff including the Head of ICT, system administrators, network engineers, cybersecurity officer and other technical support personnel whose tasks include installation, configuration, monitoring and maintenance of anti-malware systems. Secondly, the non-ICT personnel included administrative, financial, human resource, records management, healthcare and agricultural personnel. Their experience offered information regarding security awareness and user behaviour.

According to the human resource records of the County, approximately 1,200 employees in the selected departments use ICT systems on daily or weekly basis. This population constituted the sampling frame. Target population and sampling frame. The population was the [1,200] county employees who use ICT systems daily or weekly (including 28 technical ICT staff) as listed in HR Department records dated 232rd March 2025.

Inclusion criteria were employment of at least three months and use of a county computer at least weekly. Staff on leave during data collection and the 15 pilot participants were excluded.

Sampling Procedure.

Six strata were used: ICT, administration, finance, health records, agriculture and other departments (education, public works and others) as in Table 3.1. The 150 questionnaires were allocated [rule of thumb e.g. at least 20 per stratum with larger shares for departments with more ICT users]. Because allocation was not proportional [pooled results were weighted by stratum size / pooled results are unweighted and give more weight to admin & finance which is noted as a limitation]. Within each non-ICT stratum respondents were selected by simple random sampling from the numbered stratum list using [Excel RAND / SPSS random sample]; non-respondents were [not replaced].

The 20 ICT respondents were purposively selected from the 28 technical staff and [include / exclude] the four key informants. Four key informants were purposively selected for their direct responsibility for anti-malware configuration, monitoring and response. Twelve systems were purposively selected on three criteria: critical function (domain controller, file server), department coverage and product coverage (Kaspersky Endpoint Security and Windows Defender) at [headquarters / named sub-counties]

Sample Size Determination.

The regression has six predictors ($m = 6$). Green (1991) says $N \geq 50 + 8m = 98$ to test the overall model and $N \geq 104 + m = 110$ to test individual predictors. Power analysis in G*Power 3.1 (Faul et al., 2009) for medium effect ($f^2 = 0.15$), $\alpha = 0.05$, power = 0.80 and six predictors gives a minimum of 98. Allowing for 15% non-response means $110 \div 0.85 \approx 130$ questionnaires were needed. We distributed 150 (Table 3.1) and 136 returned (90.7%), which exceeds each threshold.

Response Rate and Key Informants.

Follow-ups, visits to departments and anonymity were all part of the support for a 90.7% response rate. Four key informants were interviewed: [the Head of ICT two system administrators one network security officer] because they are the post holders responsible for anti-malware configuration and response and no larger group exists. The sample is therefore based on role coverage and information power (Malterud et al., 2016) rather than on the 8–12 interviews Guest et al. (2020) found sufficient for homogeneous groups. Transcripts were reviewed after each interview and no new codes emerged after the fourth. Small number admitted as limitation (Section 6.6).

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**	

Instruments for the Collection of Data.

According to the research design, three instruments were used in order to obtain complementary data for the study: structured questionnaire, semi-structured interview guide and technical audit checklist. These instruments were developed systematically in accordance with the needs of collecting data relevant to the research objectives. Perceived effectiveness (dependent variable in regression) was measured by the PEI which is the mean of [n] questionnaire items on detection capability, response timeliness, system reliability and satisfaction (five-point Likert scale; Cronbach's alpha = 0.82). Technical effectiveness was assessed separately through audit indicators (Table 3.2). It was not entered into the regression since only 12 systems were audited. The two are compared in Table 4.14

Structured Questionnaire

Indicator	Measurement	Source	Unit
1. Detection	Internal detection rate = threats detected and recorded by the installed product ÷ [all threats identified, state denominator] × 100; independent detection rate from [scan tool, version]; zero-day share = zero-day detections ÷ total detections; false positives = count	Console logs; independent scan	%, count
2. Prevention	Real-time protection coverage = systems with it enabled ÷ systems audited; auto-resolution rate = incidents resolved without manual action ÷ incidents; repeat infections from the same source	Audit checklist; logs	%, count
3. Incident frequency	Detections per system per period = total detections ÷ systems audited; county incident count; respondent-reported incidents (Table 4.13)	Logs; ICT Department incident report; questionnaire Section C	Count, per system
4. Response time	Mean time from detection to containment [state start and stop events]; months since the response plan was last reviewed	Incident records; checklist	Hours, months
5. Update practices	Share of systems with auto-update, cloud intelligence, fully updated OS, patched third-party applications and automatic patching; share of critical vulnerabilities patched within the recommended time	Audit; vulnerability scan	%
6. User awareness	Mean of the [n]-item awareness scale (1–5; α = 0.78); share aware of the county security policy	Questionnaire	Mean, %
7. Perceived effectiveness	Perceived Effectiveness Index (PEI) = mean of [n] items on detection capability, response timeliness, system reliability and satisfaction (1–5; α = 0.82)	Questionnaire	1–5

Table 3.2: Operationalization of Variables for the set Objective Two

The structured questionnaire was used to collect quantitative data from county employees concerning their knowledge of malware threats, malware incidents, perception of anti-malware effectiveness, and challenges associated with the implementation. The questionnaire contained six sections.

Section A provided demographic and occupational information concerning the role of respondents, their tenure and department. This information helps to identify differences in staff experiences and perception of cybersecurity threats.

Section B was used to identify the self-assessed knowledge of malware using five-point Likert scale, frequency of exposure to malware threats and types of encountered malware. Section C was dedicated to the anti-malware measures used, including the use and types of anti-malware software, its effectiveness, detected and solved incidents over the last year, as well as satisfaction with system performance.

Section D covered gaps and challenges related to the implementation of anti-malware solutions, including lack of training, financial challenges, problems related to the performance of the system and difficulties in updating the system. Section E asked respondents about their suggestions on how to increase the efficiency of malware prevention and their confidence in the ability of the county to respond to malware attack. Section F allowed providing additional comments not covered in the other sections of the questionnaire.

The questionnaire included mostly close-ended questions with predetermined answers for ease of quantitative analysis and some open-ended questions. Development of the instrument adhered to the established survey design principles that include clarity, relevance, and logical sequence of questions in order to reduce errors (Fowler, 2014). The cognitive interviewing helped to identify potential problems with comprehensibility of the questions and to make the appropriate adjustments in the measurement of constructs. Five-point Likert scale was used due to its sufficient variability and clarity for respondents (DeVellis & Thorpe, 2021).

Semi-Structured Interview Guide

The semi-structured interview guide was developed to collect qualitative information from ICT and cybersecurity professionals. The guide covered the responsibilities of participants in the field of cybersecurity, types of anti-malware technologies used and reasons for choosing them, configuration and updates of systems, scan practices, history of incidents, detection of malware, response time, implementation challenges, strengths and weaknesses of the system, as well as recommendations on improvement.

Questions were designed in such a way to stimulate further discussion and allowed the participants to raise any new themes. The semi-structured interview differed from fully structured interviews in its flexibility concerning the order of questions and exploration of relevant themes beyond the initial interview protocol (Merriam & Tisdell, 2016). This method was useful to collect detailed information about the experiences and opinions of the participants in their own words.

Technical Audit Checklist

Technical audit checklist was developed to provide an objective evaluation of the configuration and performance of anti-malware systems in county ICT facilities. This measure was taken to address the gap of the previous research that largely depended on perceptions without technical confirmation (Wanjiku, 2023; Njenga, 2023).The checklist included seven sections. General information on the system was collected including department, operating system, type of anti-malware product, and the license of the product. The second section was about configuration settings including real-time protection, automatic updates, frequency of updates, scheduled scan, heuristic detection, as well as use of the cloud threat intelligence.

The third section of the checklist covered reviews of system logs concerning malware incidents, automatic and manual resolution, false positive results and recurrent infections. Assessment of the incident response covered availability and currency of the response plan, capacity of the team, response times, escalation and documentation of incidents. Vulnerabilities and patch management assessment included frequency of scan, scan results, patches applied and operating system and third-party application updates.

Statistics and metrics of detection covered total number of detections, internal and independent detection rates, time of completion of scans, system performance implications and zero-day detection rates. The seventh section was dedicated to observations, strengths and weaknesses of the systems and recommendations on improvement. The checklist was filled through the direct inspection of the system, review of available logs and consultations with ICT staff. Evidence-based evaluation of the anti-malware system configuration and performance helped to reduce reliance on self-reported information and provide consistent evaluation of all

systems. This approach to cybersecurity system assessment is suggested by the National Institute of Standards and Technology (2020).

Validity and Reliability of Instruments

Validity and reliability were addressed to increase the credibility and consistency of the results. The measures were undertaken according to the established research principles (Creswell & Creswell, 2021).

Validity

Validity implies the extent to which an instrument measures what it is supposed to measure (DeVellis & Thorpe, 2021). In this study, the content, face, and construct validity were examined. Content validity was provided through development of questionnaire items, interview questions and audit checklist indicators on the basis of comprehensive review of the literature on malware threats, anti-malware effectiveness and challenges of cybersecurity implementation (Al-Duwairi & Al-Eroud, 2021; Ahmad & Khan, 2021; Patel & Soni, 2022; Wanjiku, 2023). Constructs of threat appraisal, coping appraisal, deterrence mechanisms, and technology acceptance were operationalized by the items based on previously validated measurements.

Face validity was established by the review of questionnaire, interview guide and checklist by the research supervisors – Dr. Castro Yoga and Dr. Jacob Ogweno – who had the experience in information systems and cybersecurity research. The feedback concerning the clarity, relevance and appropriateness of instruments allowed to make necessary changes before pilot testing. Although it is a subjective type of validation, it helps to understand whether the instrument looks good to measure the intended concept (Hardesty & Bearden, 2004).

Construct validity was increased due to the triangulation of questionnaires, interviews and technical audits. The convergence between the sources increased the reliability that the research constructs were measured properly. The factor analysis was intended to evaluate whether multi-item scales including perceived effectiveness, load on the expected dimensions (Hair et al., 2021).

The pilot study with 15 people (ten non-IT staff and five IT personnel) was conducted to examine the clarity, relevance, ambiguity, and duration of questionnaire items. The participants of the pilot study were excluded from the sample of the main study. Cognitive interviews helped to detect questions requiring clarifications and rewording, while iterative development improved the appropriateness of responses and decreased the time of completing the form. Also, the technical audit checklist was piloted in three systems to check its usability and item sequencing.

Reliability

Reliability is the consistency and stability of measurements if the instrument is used in the similar conditions (DeVellis & Thorpe, 2021). The internal consistency of multi-item questionnaire scales was measured using Cronbach's alpha that measures the extent to which items within a scale are interrelated (Taber, 2018). The value of at least 0.70 is considered acceptable according to Nunnally and Bernstein (1994).Perceived effectiveness scale achieved Cronbach's alpha of 0.82, user awareness scale 0.78 and policy enforcement scale 0.75. All the values were above the threshold and provided satisfactory internal consistency. The inconsistencies, if any, were addressed using item analysis of potentially problematic questions.

The inter-rater reliability was measured by auditing the four systems independently by two researchers using the technical checklist. Their findings were compared, disagreements were discussed and the audit procedure was clarified in order to avoid the subjective interpretation. Test-retest reliability was checked by administering the questionnaire to the sub-sample of eight participants of the pilot study at two-week intervals. Standardized procedures helped to increase reliability. Interview protocols provided consistent structure allowing necessary flexibility. Technical audit items were defined precisely to reduce differences in their interpretation.

Trustworthiness of Qualitative Elements

Trustworthiness of interviews and open-ended survey responses was evaluated using the framework developed by Lincoln and Guba (1985) and including criteria of credibility, transferability, dependability and confirmability. Credibility was increased due to triangulation of interviews, questionnaires, and technical audit findings. Member checking allowed key informants to review summaries of their contributions and clarify interpretations. Peer debriefing provided by regular discussions with research supervisors gave an opportunity to question assumptions and refine interpretations.

Transferability was facilitated by detailed descriptions of Homa Bay County Government, participants, research procedures and analysis methods that allows readers to evaluate the relevance of the findings in other settings. Dependability was enhanced through audit trails of research decisions, data collection and analysis procedures. Confirmability was increased through reflexivity. The researcher kept the journal describing his assumptions, possible biases and reflections during the entire research process. The triangulation helped to provide evidence from various sources for the interpretations instead of researcher's perspective.

Data Collection Methods

Data collection took eight weeks starting from early April 2025 to late May 2025. The surveys, semi-structured interviews and technical audits were used to collect complementary data relevant to the research objectives.

Data Source	Population/Sample	Instrument	Variables Covered	Analysis
Questionnaire	136 county employees	Structured questionnaire (Section C)	Installation, products, perceived effectiveness, incidents, satisfaction, predictors of effectiveness	Descriptive and regression
Interviews	4 ICT key informants	Semi-structured interview guide	Configuration, licensing, tools, practice across departments	Thematic analysis
Technical audit	12 systems	Audit checklist and system logs	Configuration, detection, response, patching, performance	Descriptive

Table 3.3: Data Sources and Their Contributions

Survey Administration

Prior to the data collection, the researcher gained the permission to conduct the study in Homa Bay County Government via the introductory letter from Great Lakes University of Kisumu. The County ICT Department helped to identify departmental contacts who helped to gain access to the sampled employees. Each questionnaire was sent together with the cover letter explaining the aim and significance of the study and arrangements for confidentiality.
The respondents completed the questionnaire immediately or within an agreed upon time period that usually takes two to three days. The researcher visited the respondents to collect completed questionnaires and clarify questions. Those who preferred electronic participation were sent a Google Forms link by email.

The mixed mode administration allowed maintaining the consistency of questionnaire content and allowing different preferences of respondents. The De Leeuw (2018) notes that the mixed mode surveys can be beneficial when properly managed. The researcher recorded all the procedures related to the survey

distribution, responses and follow-ups. Of 150 questionnaires distributed, 136 were returned, achieving response rate of 90.7%. Of the 136 returned questionnaires [n] were filled in on paper and [n] through Google Forms.

Interviews with Key Informants

The semi-structured interviews were conducted with four purposively selected key informants the Head of ICT, two system administrators and one network security officer. The purposive sampling was used in order to identify the staff members involved in cybersecurity operations and knowledgeable about anti-malware deployment, incident history, and operational challenges. The interviews were scheduled in the convenient place, usually in the office or county headquarters, and took 45-75 minutes. Upon agreement with the participants, the interviews were recorded and some notes were taken for capturing the non-verbal information and context of the conversation.

The semi-structured interviews allowed the researcher to follow the interview guide and explore emerging themes. At the end of each interview, the key points and preliminary interpretations were reviewed to inform the next interview. The recording was transcribed verbatim within 48 hours to maintain the accuracy and context of the conversation.

Technical System Audit.

Twelve systems were purposively selected: two servers (a domain controller and a file server) and ten workstations from ICT, finance, administration, health records and agriculture departments (Table 4.6). Visits took place over 14 days. For each system the researcher recorded configuration settings from product console and configuration files; reviewed six months of logs (Table 4.9); took 12-month detection totals (Table 4.8) from [console statistics]; patch status and last vulnerability scan from. Response and policy documents were checked against checklist (Appendix B). Exploitation or penetration testing was not done.
.
System logs covering the period of six months were reviewed to detect malware detections, automatic and manual resolutions, false positives and recurrent infections. Patch status of the operating system and third-party applications and vulnerability scan results were examined. Detection and performance statistics were obtained from the anti-malware management console if available and were compared to the independent scan findings. Incident response plans, security policies, and documentation were also reviewed. The findings were recorded in the audit checklist and screenshots of configuration screens were taken with the permission.

Then, the findings were discussed with ICT staff to verify accuracy and clarify technical issues.
The combination of surveys, interviews and technical audit provided triangulation. The surveys gathered the experience and perception of the employees, interviews provided insights from specialists on technical and organizational issues and audits provided the evidence on system configuration and behaviour
.

Ethical Considerations

The ethical approval of the Great Lakes University of Kisumu Ethics Review Committee and research license from the National Commission for Science, Technology and Innovation (NACOSTI) were obtained.

Informed Consent

Participants were informed about the aim of the study, procedures, voluntary participation, potential risks and benefits, confidentiality arrangements and their right to withdraw without penalty. Survey respondents received this information in a cover letter, while returning of the completed questionnaire means the consent to participate. Interview participants signed the detailed consent forms after receiving the information about the study.

Confidentiality and Anonymity

Confidentiality was provided through several measures. Survey respondents were not asked for their names. Interview participants were given pseudonyms, identifying details were removed from transcripts and the final report. Paper records were stored in locked cabinets and electronic files were protected with password encryption. Access was limited to the researcher and supervisors. The results were presented using the aggregated data and anonymized quotes to prevent the identification of individuals.

Organizational Consent and Access

Authorization to conduct the study was obtained from Homa Bay County Government after sending an introductory letter from Great Lakes University of Kisumu and research proposal to the County Secretary and Chief Officer for ICT. The authorization provided access to the relevant staff and ICT systems.

Data collection was planned in order to minimize the disruption to county operations. The interviews were arranged considering participants' working schedule, and audits were carried out during the period of low activity. No penetration testing or exploitation of vulnerabilities was performed. Assessment was conducted with the help of already existing configurations and logs without affecting system stability and availability.

Data Security and Privacy

As a result of the sensitivity of the data on cybersecurity, all system logs and configuration information were treated with caution. Records were stored safely and all identifying data such as IP address and name of the system were removed during processing. Information was presented on the aggregated level without revealing any system vulnerabilities.

Value and Benefits of the Study

Even though the study was conducted in academic purposes, it aimed to provide value for the host organization. Summary report with findings and recommendations will be provided to Homa Bay County Government. In this way the principle that research should add value to the organizations was reflected
.

Limitations of the Study

There are several limitations of the study which should be taken into account while interpreting the results. First of all, the single-case study limits the possibility to make statistical generalizations to other Kenyan county governments. However, the results provide valuable contextual insights for similar institutions. According to Yin (2018) case studies provide detailed understanding of particular context although they cannot be generalized out-of-hand to other cases. Secondly, cross-sectional design provides information about a particular period of time and does not allow establishing the causality between anti-malware practices and effectiveness. Regression analysis provides associations but not causation.

Third, the technical audit covers only 12 systems out of about 1200 county systems. So, the results give indication of system conditions rather than assessment of whole county ICT environment. Fourth, there can be selection bias as a result of stratified random sampling used for the survey and purposive selection used for conducting interviews and technical audit. Respondents who agreed to participate can differ from those who declined to participate, while systems audited may not be representative of county's ICT environment. Information about sampling strategy and participants helps reader to consider this limitation.

Fifth, technical logs, incident records and configuration information can be incomplete and inconsistent due to limitations in resources and time. Sometimes historical incident records in some systems were limited which can affect the quality and precision of technical audit. Comparison of information provided from different sources reduced this limitation. Sixth, malware threat landscape is changing very fast due to new attacks,

modified variants of malware and zero-day threats. The findings may not take into account changes occurred after collecting the data in April and May 2025.

Seventh, the technical audit assessed the current configurations and logs but did not perform any controlled penetration testing or simulation of zero-day attacks. So, detection capabilities of the system against new threats were not assessed. Signature-based anti-malware technologies cannot detect newly developed, polymorphic or fileless malware. Thus, the effectiveness was assessed according to detection records, configurations and historical practices rather than by experiments.

Eighth, self-reports provided during survey and interviews may suffer from recall bias and social desirability bias. Respondents can overestimate their knowledge and underestimate the number of incidents because of embarrassment or fear of consequences. Anonymity, confidentiality, objectivity and triangulation of information helped to reduce these biases.
Ninth, resource limitation and shortage of cybersecurity specialists may affect anti-malware technologies deployment and incident management. These factors can also affect availability of employees and quality of documentation during data collection. The researcher planned activities flexibly in order to avoid any interruption.

Finally, changes in national cybersecurity policies, institutions arrangements and cooperation among agencies can affect the relevance of the findings. However, the study used multiple sources of data, structured sampling, validated measurement tools and transparency in reporting which helped to increase confidence in findings and their relevance to anti-malware capacity in Kenyan county governments.

Data Analysis

Quantitative Analysis; Questionnaires were checked for completeness: fewer than 2% of values were missing and were dealt with by [listwise deletion / mean substitution]. Data were coded and analysed in SPSS version 27. Multiple linear regression (enter method, two-tailed $\alpha = 0.05$) regressed the Perceived Effectiveness Index on the six predictors. Assumptions were checked as follows: linearity (scatterplots of standardised residuals against predicted values), normality of residuals (histogram and P–P plot), homoscedasticity (residual plot), multicollinearity (VIF < 5; maximum [value]), independence (Durbin–Watson = 1.89) and influential cases (maximum Cook's distance [value], below 1). Since outcome and most predictors came from one questionnaire common-method bias was checked with [Harman's single-factor test; first factor explained [%] of variance] (Podsakoff et al., 2003). Results report B with 95% CI, β, t, p, R^2, adjusted R^2 and $F(6, 129)$.

Qualitative Analysis: Transcripts of interviews were analysed using thematic analysis and Braun and Clarke's (2006) six-phases approach: becoming familiar with data, initial coding, searching for themes, reviewing themes, defining themes and reporting findings. Coding was performed deductively according to theoretical framework and inductively by identifying emerging themes. Two researchers independently coded part of transcripts and discussed differences to increase consistency. Transcripts were coded in [NVivo / Excel]. Two researchers coded [%] of transcripts independently with agreement [% / κ]; discrepancies were discussed, codebook is in Appendix [D].

Technical Audit Analysis: Results of technical audit were recorded using checklist and analysed with the help of descriptive statistics such as frequencies, percentages and means. Detection rates were calculated based on system logs where denominator data was available. If needed information was not available, this limitation was stated. Results of technical audit were compared to survey and interview results to increase understanding of anti-malware effectiveness.). Internal detection rate was [number of threats recorded as detected and handled in console logs / total threats identified in the logs] for each system and pooled; for independent check scan tool, version, definition date was run on all 12/n systems read only, results compared with console records; independent rate is define: share of threats found by independent scan that were also found by installed product. Zero-day detections were those classified as such by product's own threat report.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue X October 2026

RESULTS AND FINDINGS

Introduction

This chapter presents findings related to the research objective – evaluation of anti-malware security technologies effectiveness implemented in Homa Bay County Government. The results are organized around respondent characteristics, anti-malware technologies deployed, technical audit results on configuration, detection, incident response and patching, perception of respondents about effectiveness, comparison of perceived and technical effectiveness, regression analysis and findings from interviews with key informants.

The target group of the study included 150 participants among estimated population of 1200 employees who work with ICT systems in Homa Bay County government departments. From 150 questionnaires distributed 136 questionnaires were returned. Response rate was 90.7%. Quantitative data was analysed using SPSS software, while interview data was analysed using thematic analysis. Results of technical audit were analysed using descriptive statistics. Three sources of data were integrated to complement survey results.

Response Rate and Respondent Profile

Questionnaire Distribution and Return Rate

In total 150 questionnaires were distributed to the selected employees of Homa Bay County Government departments. 136 of them were returned which gave response rate of 90.7%. 14 questionnaires were not returned and constituted 9.3% non-response. The response rate provided a good ground for quantitative analysis and was supported by systematic distribution of questionnaires, follow-ups and assurance of confidentiality. Returned questionnaires became the base for analysis of respondents' experience, perceptions and assessment of anti-malware technologies deployed in the county.

Department/Stratum	Distributed	Returned	Response Rate (%)
ICT Personnel	20	18	90.0 %
Administrative Employees	35	32	91.4 %
Finance Staff	30	28	93.3 %
Health Records Staff	25	23	92.0 %
Agricultural Staff	20	17	85.0 %
Other Departments	20	18	90.0 %
Total	**150**	**136**	**90.7 %**

Table 4.1: Questionnaire Distribution and Return Rate

The total response rate of 90.7% (see Table 4.1 below) far exceeds the 70% threshold considered excellent in social science research (Mugenda & Mugenda, 2012). This was ensured through continuous follow-ups and visits to departmental offices and through assurance of confidentiality. All strata had a response rate of 85% and above, meaning all main departments are represented in the sample.

Data Quality

A number of steps were taken to ensure data quality. The survey instrument was pre-tested on 15 respondents (10 non-IT staff and 5 ICT personnel). Cognitive interviewing of the respondents in the pilot group helped to

identify any ambiguous items. The survey was conducted in a uniform manner across all departments. Checks were conducted on completeness and consistency of the completed questionnaires and less than 2% of the responses were missing; these were resolved during the data cleaning stage. Survey results were triangulated with the interview and technical audit evidence.

Length of Service Distribution

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 %**

Table 4.2: Length of Service in the Current Job

From Table 4.2 above, it is clear that 61.7% of respondents have worked in the County for more than four years (38.2% have been working for 4-6 years and 23.5% for more than 6 years). Therefore, most respondents are experienced employees familiar with the ICT infrastructure and security procedures in the County. 13.2% have been working for less than one year, which means that respondents have sufficient knowledge of the organization to answer the survey questions correctly.

Distribution of 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 %**

Table 4.3: Respondents by Department

The departmental distribution in Table 4.3 above reflects the stratified sampling design explained in Chapter Three. The largest proportions were Administration (23.5%) and Finance (20.6%) followed by Health Records (16.9%), the ICT Department (13.2%), Other Departments (13.2%) and Agriculture (12.5%). This means that technical and non-technical users of the County's ICT systems are fairly represented.

Anti-Malware Technology Deployment

Anti-Malware Software Installation Rate

Anti-Malware Installed	Frequency (n)	Percentage (%)
Yes	116	85.3 %
No	12	8.8 %
Not sure	8	5.9 %
Total	**136**	**100 %**

Table 4.4: Anti-Malware Software Installation Status

As is shown in Table 4.4 above, most respondents (85.3%) report that anti-malware software is installed on their work computers. However, 8.8% report that it is not installed and 5.9% report that they are not sure, which means that there are either coverage gaps or insufficient knowledge of the tools available. The technical audit revealed that anti-malware software is installed on all 12 audited systems, thus the gap in the survey can be attributed to at least in part, to users being unaware of the presence of the protection tools on their computers.

Anti-Malware Software in Use

The respondents who reported having the software installed (n=116) were asked to name the product used.

Anti-Malware System	Frequency Mentioned (n)	Percentage of Respondents (%)
Windows Defender for Endpoint	72	62.1 %
Kaspersky Endpoint Security	48	41.4 %
Malwarebytes	26	22.4 %
Symantec Endpoint Protection	18	15.5 %
Avast/AVG	12	10.3 %
Other	8	6.9 %

Table 4.5: Anti-Malware Software Used (multiple answers)

Windows Defender for Endpoint (62.1%) was the most popular product used, due largely to the fact that it is included in the Windows operating system. Kaspersky Endpoint Security (41.4%) was used predominantly on the systems managed by the ICT Department.

The deployment of multiple products throughout the County, as can be seen from Table 4.5 above, increases the complexity of management and monitoring of the anti-malware solutions.

Systems Covered by the Technical Audit

System ID	Type	Department	Operating System	Anti-Malware Software
SVR-01	Server	ICT	Windows Server 2019	Kaspersky Endpoint Security 12
SVR-02	Server	ICT	Windows Server 2016	Kaspersky Endpoint Security 12
WS-01	Workstation	ICT	Windows 10 Pro	Windows Defender
WS-02	Workstation	ICT	Windows 10 Pro	Kaspersky Endpoint Security 12
WS-03	Workstation	Finance	Windows 10 Pro	Windows Defender
WS-04	Workstation	Finance	Windows 10 Pro	Windows Defender
WS-05	Workstation	Finance	Windows 10 Pro	Kaspersky Endpoint Security 12
WS-06	Workstation	Administration	Windows 10 Pro	Windows Defender
WS-07	Workstation	Administration	Windows 10 Pro	Windows Defender
WS-08	Workstation	Health Records	Windows 10 Pro	Windows Defender
WS-09	Workstation	Health Records	Windows 10 Pro	Windows Defender
WS-10	Workstation	Agriculture	Windows 10 Pro	Windows Defender

Table 4.6: Systems Covered by the Technical Audit

2 servers and 10 workstations were selected purposively from the ICT, Finance, Administration, Health Records and Agriculture departments. Kaspersky Endpoint Security (version 12) was installed on both servers and 2 workstations and Windows Defender was installed on 8 workstations.

Technical Audit: Anti-Malware Solution Configuration

Configuration Parameter	Compliant Systems (n)	Total Systems	Compliance Rate (%)
Real-time protection enabled	12	12	100 %
Auto-update of definitions enabled	10	12	83.3 %
Scheduled scans configured	8	12	66.7 %
Heuristic/behaviour detection enabled	9	12	75.0 %
Cloud threat intelligence enabled	10	12	83.3 %

Table 4.7: Anti-Malware Solutions Configuration Audit Results

The following were the key findings related to the configuration of the tools (see Table 4.7 above):
All 12 systems had real-time protection enabled, which means that basic protection was consistently applied;
All but two out of 12 systems had auto-update enabled (83.3%);
Only 8 out of 12 systems (66.7%) had scheduled scans configured, four workstations had real-time protection only;

Heuristic detection was enabled on 9 out of 12 systems (75.0%), it was disabled on 3 systems due to the possibility of false positives;
Cloud threat intelligence was enabled on 10 out of 12 systems (83.3%), which allows faster updates on emerging threats.

Technical Audit: Anti-Malware Solutions Performance
System Logs and Detection Performance

Metric	Finding
Total malware detections (12 months)	**42**
Detection rate: internal logs	95%
Detection rate: independent scans	88%
Average scan completion time (quick scan)	15 minutes
Average scan completion time (full scan)	90 minutes
Impact on system performance during scans	Moderate
Zero-day threats detected	3 (7% of total threats)

Table 4.8: Detection Statistics and Performance Metrics

Forty-two malware detections were recorded on the 12 systems over 12 months; internal logs showed 95% detection and independent scan 88%. Since the two sources disagree, the internal figure is best read as product record and independent figure as cross check.

Quick scans took about 15 minutes, full scans about 90 minutes — users reported noticeable slowdowns during full scans. Of the 42 detections three (7.1%) were zero-day threats — no controlled zero day test was run (3.10) so this shows what was detected rather than missed; consistent with but not proof of limited detection of unknown malware.

Metric	Findings
Logs available for past 6 months	12 of 12 systems
Total malware incidents detected	**24 incidents**
Automatically resolved incidents	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)

Table 4.9: System Logs Audit Results (6-Month Period)

The six-month period audit of logs (see Table 4.9 above) revealed that 83.3% of 24 incidents were resolved automatically, which is indicative of the good performance of the tools in resolving routine threats. Four incidents needed a manual intervention and two cases of repeated infection from the same source of phishing were observed.

Incident Response Capabilities

Parameter	Finding
Documented incident response plan exists	Yes
Last reviewed/updated	10 months ago
Designated incident response team available	Yes
Average response time to detected threats	2 hours
Escalation procedures followed	Yes
Containment, eradication and recovery records	Yes

Table 4.10: Incident Response Audit Results

The ICT Department has a written procedure for the incident response; however, it has not been reviewed in the last ten months prior to the audit. A team consisting of the Head of ICT, System Administrator and Network Security Officer is designated, the response time of about two hours on average is reasonable but can be improved through automation and documentation of the incident containment, eradication and recovery is satisfactory (see Table 4.10 above).

Vulnerability Scanning and Patch Management

Parameter	Finding
Frequency of vulnerability scans	Quarterly
Last scan date	2 months ago
Critical vulnerabilities found in last scan	6
Patched within recommended time frame	83 %
Operating system fully updated	10/12 systems (83.3%)
Third-party applications patched	8/12 systems (66.7%)
Automatic patch management enabled	9/12 systems (75.0%)

Table 4.11: Vulnerability Scans and Patch Management Audit Results

Vulnerability scanning is done on a quarterly basis. Six critical vulnerabilities were found in the last scan, of which 83% were patched within the recommended time. Operating system patches are up-to-date on 10 out of 12 systems (83.3%), but the two exceptions are servers on which updates are intentionally delayed until stability testing. Third-party application patches are weaker – only 8 out of 12 systems (66.7%) are fully patched, which is important since browsers, PDF readers and office suites are among the most common targets for malware (see Table 4.11 above)

4.6. Users' Perceptions of Effectiveness

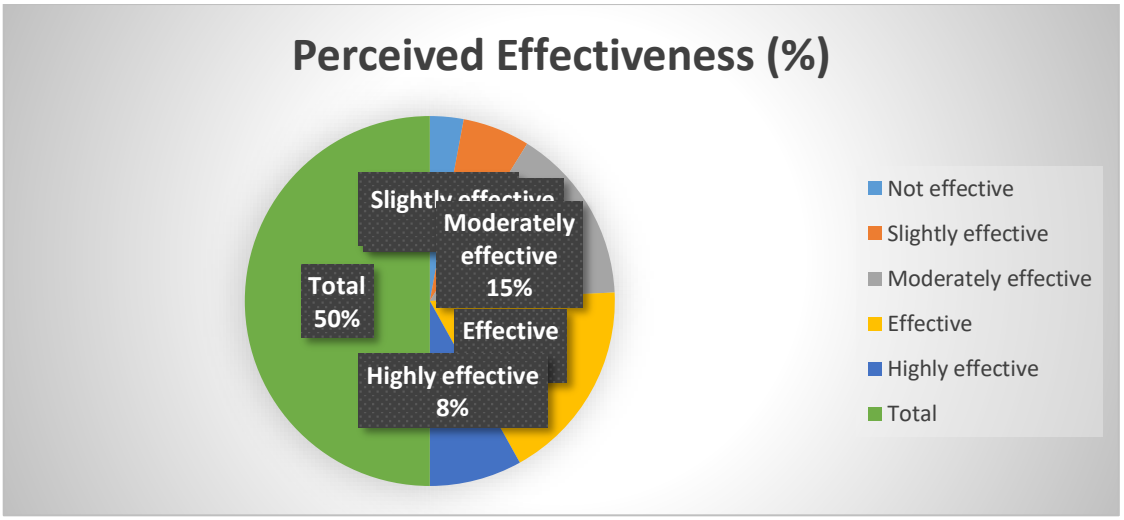


Chart4.1: Perceived Effectiveness of Anti-Malware Systems

Respondents rated the effectiveness of the current anti-malware systems on a scale from 1 (not effective) to 5 (highly effective). The average rating was 3.44. As Table 4.12 above shows, 82.4% of respondents rated effectiveness as moderate or higher (30.9% as moderate, 35.3% as effective and 16.2% as highly effective), whereas 17.7% of respondents rated effectiveness as low. Thus, users are generally confident in the current anti-malware tools.

Awareness measure	Result
Mean awareness score (1–5), SD	[mean], [SD]
Aware of the county cybersecurity policy	[30.9%]
Received anti-malware or security training in the past 12 months	[%]
Cited outdated software or signatures as a limiting factor	[60.3%]

Table 4.12. User Awareness

User awareness was measured by a [n]-item scale (mean [value], SD [value], $\alpha = 0.78$). Table 4.12a shows that [30.9%] of respondents were aware of the county cybersecurity policy and [60.3%] named outdated software or signatures as limiting factor.

Incidents Detected	**Frequency (n)**	**Percentage (%)**
0	10	7.4 %
1–5	68	50.0 %
6–10	32	23.5 %
More than 10	12	8.8 %
Not sure	14	10.3 %
Total	**136**	**100 %**

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue X October 2026

Table 4.13: Number of Incidents Detected and Mitigated in the Past Year (Respondents' report

Half of the respondents (50.0%) reported that their systems had detected and mitigated 1-5 incidents in the past 12 months, 23.5% reported 6-10 and 8.8% reported more than ten, but 7.4% reported no incidents at all (Table 4.13). This means that malware is a regular phenomenon and existing anti-malware tools detect at least some of the infections.

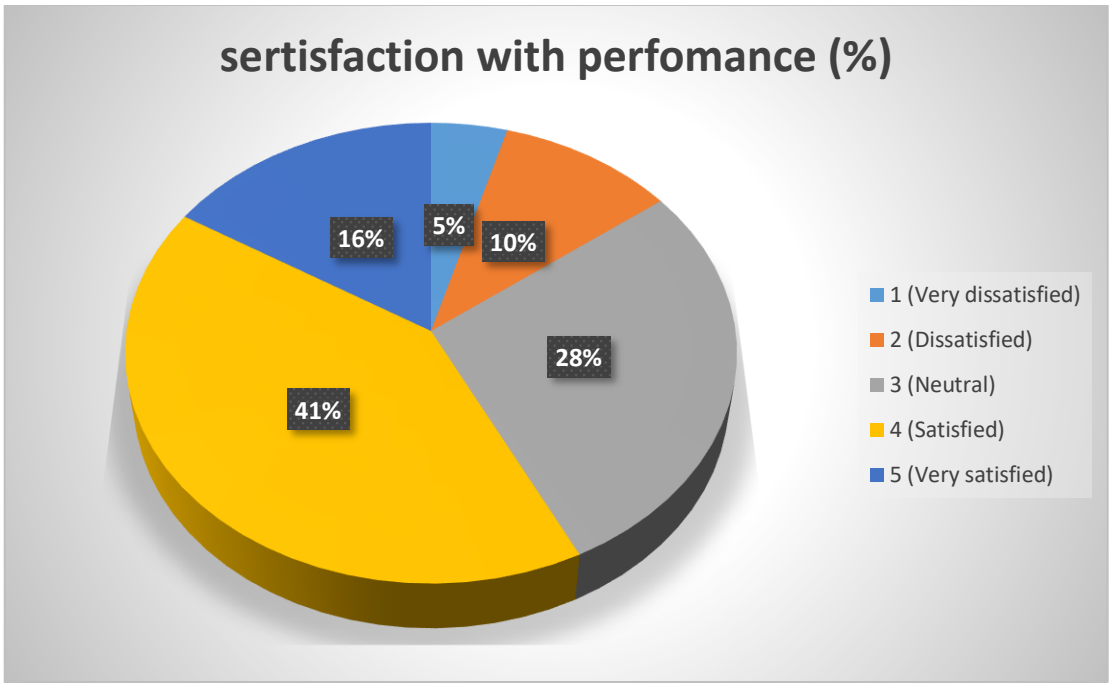


Chart 4.2: Satisfaction with Anti-Malware Systems Performance

More than half of respondents (57.4%) were either satisfied (41.2%) or very satisfied (16.2%) with the performance of the systems, and 14.7% were dissatisfied. The average satisfaction score was 3.54. This is possibly due to the preference for visible security features, such as alerts and automatic scans, despite the technical deficiencies revealed by the audit.

Perceptions vs. Technical Evidence

Aspect	**User Perception**	**Technical Reality**
Overall effectiveness	82.4% rated effectiveness as moderate to high	Detection rate of 88–95% for known threats, but only 7% of detections were zero-day
Update practices	60.3% cited outdated software or signatures as a limiting factor	83.3% auto-update compliance, but servers updated manually and third-party patching weak (66.7%)
System protection	Users generally confident in the protection	Real-time protection on 100% of systems, but scheduled scans missing on 33.3%
Threat landscape	Aware of common threats	Persistent infections confirmed by logs

Table 4.14: Perception vs. Technical Reality

From Table 4.14 above, it is clear that users' perceptions are more positive than the technical evidence shows. This means that users' confidence is based on visible security features, such as alerts, notifications and automatic cleaning, but not on the resilience of the system against complex threats.

Factors Associated with Anti-Malware Effectiveness: Regression Analysis

Model Specification

Multiple linear regression was used to explore the relationships between six independent variables and anti-malware effectiveness. The regression equation is as follows:

Effectiveness = $\beta_0 + \beta_1$(Training) + β_2 (Patch Management) + β_3 (Technology Type) + β_4 (User Awareness) + β_5 (Policy Enforcement) + β_6 (Resource Allocation) + ε

Dependent variable was a composite score of questionnaire items on detection, response, reliability and satisfaction with the systems (Cronbach's α=0.82). Independent variables were staff training (frequency and quality of cybersecurity training), patch management (consistency and timeliness of patches), type of anti-malware technology (signature-based vs. advanced or AI-based), user awareness (security scores and behaviours), policy enforcement (awareness and enforcement of security policies) and resource allocation (cybersecurity budget).

Regression Results

Model	**R**	**R^2**	**Adjusted R^2**	**Std. Error**
1	0.782	0.612	0.594	0.423

Table 4.16: Model Summary

As can be seen from Table 4.16 above, R=0.782 and R^2=0.612, meaning that the six independent variables account for 61.2% of the variance in anti-malware effectiveness.

Source	**SS**	**df**	**MS**	**F**	**Sig.**
Regression	42.36	6	7.06	33.94	< 0.001
Residual	26.84	129	0.208		
Total	**69.20**	**135**			

Table 4.17: ANOVA Results

F-statistic is 33.94 (ratio of mean square of regression, 7.06, to mean square of residuals, 0.208), $p<0.001$ (Table 4.17 above). The model is thus statistically significant.

Predictor	B	Std. error	95% CI for B	Beta	t	Sig.
(Constant)	1.234	0.342	0.557 to 1.911		3.608	< 0.001
Staff training	0.412	0.086	0.242 to 0.582	0.356	4.791	< 0.001
Patch management	0.378	0.092	0.196 to 0.560	0.312	4.109	< 0.001
Technology type	0.156	0.078	0.002 to 0.310	0.142	2	0.047

User awareness	0.224	0.084	0.058 to 0.390	0.198	2.667	0.009
Policy enforcement	0.142	0.076	−0.008 to 0.292	0.128	1.868	0.064
Resource allocation	0.168	0.082	0.006 to 0.330	0.146	2.049	0.042

Table 4.18: Regression Coefficients with 95% confidence intervals

Interpretation of Regression Results

Staff training had the highest standardised coefficient (β = 0.356, p < 0.001; B = 0.412, 95% CI 0.242–0.582) so that for every one unit increase in the training score there was a 0.412 unit increase in the effectiveness score holding other variables fixed. Patch management was the second strongest predictor (β=0.312, p<0.001). User awareness (β=0.198, p=0.009), resource allocation (β=0.146, p=0.042) and technology type (β=0.142, p=0.047) were statistically significant but weaker predictors. Policy enforcement (β=0.128, p=0.064) was not statistically significant at 5% level. This does not mean that policy enforcement has no effect, but rather the data are not providing enough evidence of its effect at the conventional level.

A major limitation here is that these are associations in a cross-sectional design; thus, this regression just helps to identify factors associated with effectiveness and does not prove causality.

Key Informants' Interviews: Technologies

There were two themes in key informants' interviews which relate to the deployed technologies. First, resource constraints dictate what technologies are selected by the County, so that it relies on signature-based products:

"We would love to deploy AI-based endpoint detection and response tools, but they are really expensive. We have to make do with what we've got – almost all signature-based tools – and hope for the best." – KI-01
"There are times if we cannot renew licenses on time because of delays of procurement. We've had periods when systems ran on expired definitions." – KI-04

Second, there are variations in practices across departments and there is no central mechanism of enforcement:
"Some departments are very good about updates and following our guidelines. Others are not. We don't have a way to enforce compliance centrally." – KI-01

"We've found systems in the health department that hadn't been updated in six months. They said they were too busy with patient data entry to allow updates." – KI-03

Auditor's Observations

The auditor highlighted the following strengths in the deployed technologies: all systems have valid, licensed anti-malware software; real-time protection is enabled on all systems; there is an active incident response team with defined responsibilities; documentation of incidents and logs is well maintained; quarterly vulnerability scans are performed. Limitations are the following: Inconsistent auto-update policy, as two servers depend on manual updates;

No scheduled scans on four systems (33.3%);Insufficient third-party application patching: only 66.7% of systems are fully patched;

Limited zero-day threat detection due to reliance on signature-based detection; Fragmented management, without central monitoring across the departments.

Summary of Key Findings on the Effectiveness of Technologies

Area	Key Finding
Coverage	85.3% of respondents report installation; 100% of audited systems have anti-malware installed
Products	Windows Defender (62.1%) and Kaspersky (41.4%) most common; several products in use
Configuration	Real-time protection 100%; auto-update 83.3%; cloud intelligence 83.3%; heuristic detection 75.0%; scheduled scans 66.7%
Detection	95% (internal logs) versus 88% (independent scans); zero-day detections 7% of total
Patching	OS fully updated 83.3%; third-party applications 66.7%; automatic patching 75.0%
Perception	82.4% rate effectiveness moderate to high; 57.4% satisfied
Determinants	$R^2 = 0.612$; training ($\beta = 0.356$) and patch management ($\beta = 0.312$) strongest predictors

Table 4.19: Summary of Key Findings on the Effectiveness of Anti-Malware Technologies

Dimension	Indicator	Value	Rating
Detection	Internal detection rate	95%	High
Detection	Independent-scan detection rate	88%	Moderate
Detection	Zero-day share of detections	3 of 42 (7.1%)	Not rated: no zero-day test
Prevention	Real-time protection enabled	12 of 12 (100%)	High
Prevention	Incidents auto-resolved	20 of 24 (83.3%)	Moderate
Prevention	Repeat infections (phishing source)	2 cases	Not rated
Incident frequency	Detections per system per year	3.5	Not rated
Response	Mean response time; plan last reviewed	2 hours; 10 months before audit	Not rated
Update practices	Auto-update of definitions	83.30%	Moderate
Update practices	Cloud threat intelligence	83.30%	Moderate
Update practices	Heuristic detection enabled	75.00%	Moderate
Update practices	Scheduled scans configured	66.70%	Low
Update practices	Operating system fully updated	83.30%	Moderate
Update practices	Third-party applications patched	66.70%	Low

Update practices	Automatic patch management	75.00%	Moderate
Update practices	Critical vulnerabilities patched on time	5 of 6 (83%)	Moderate
Perception	Rated moderate or higher; mean 3.44 of 5	82.40%	For comparison only

Table 4.20. Technical Effectiveness Score card

Of the 12 rated indicators 2 were high, 8 moderate and 2 low. The overall rating of "moderately effective" follows from this distribution; scheduled scans and third-party patching are weakest points and zero-day detection cannot be verified.

CONCLUSION

Deployed anti-malware technologies provide the County with a baseline of protection: they are installed and licensed on all audited systems, have real-time protection, automatically resolve most of routine incidents and are backed by an active incident response team. However, they are only moderately effective because of configuration gaps, uneven patching, fragmented solutions and the reliance on signature-based detection, which limits their effectiveness against new and sophisticated malware. Users' confidence exceeds the technical evidence and regression results suggest that effectiveness is associated more with training and patch management than with the type of the technology

DISCUSSION

Interpretation of the Main Findings

Performance of the Anti-Malware Technologies

The findings indicate that Homa Bay County Government has established baseline anti-malware protection, but configuration weaknesses limit its performance. While 85.3% of respondents reported that anti-malware software was installed on their work computers, technical audits showed that all 12 audited systems had anti-malware protection. However, automatic updates were enabled on only 83.3% of systems, scheduled scans were configured on 66.7%, and third-party application patching was done on 66.7%. Such shortcomings are similar to those revealed by Njenga (2023) in his study of Kisumu County and by Wanjiku (2023) in her multisite study of several Kenyan county governments.

The audit recorded 42 detections were recorded in the audit (3 zero-day threats out of 7.1%). Patel and Soni (2022) found that signature tools detect 23–45% of zero-day samples, heuristic and machine learning tools 62–78%. Low zero-day count here is consistent with that pattern but only indicative because this study didn't test zero-day samples. Windows Defender and Kaspersky both have heuristic, behavioural and cloud assisted engines. In the audit they were off or absent on some systems (heuristic detection on three, cloud intelligence on two), informants described estate mostly signature based. The limit on detecting novel polymorphic fileless malware (Al-Duwairi & Al-Eroud, 2021) therefore appears to come from configuration and licensing rather than product capability alone (a point that a controlled test should prove)..

While 82.4% of respondents evaluated effectiveness of anti-malware technologies as moderate or high and 57.4% said they were satisfied with system performance, there were technical gaps identified during the audit. From the point of view of TAM, users perceive the technologies as useful because they see alerts, notifications, and automatic cleaning actions performed by the software. However, such visibility does not imply protection against sophisticated threats. The perceived usefulness in the mandatory-use environment can be based on very limited information; therefore, an independent technical evaluation is required.

Factors Associated with Effectiveness

The multiple regression model showed that the six independent variables explain 61.2% of variance in anti-malware effectiveness ($R^2 = 0.612$).

Training was the strongest predictor ($\beta = 0.356$, $p < 0.001$). The finding supports the PMT, which states that coping appraisal is related to self-efficacy and response efficacy. Training increases employees' confidence that they will be able to conduct protective behaviour and that this behaviour is effective. The finding confirms Ifinedo (2012) and Boss et al. (2015) stating that training and awareness increase security compliance and protective behaviour.

Patch management was the second-strongest predictor ($\beta = 0.312$, $p < 0.001$). The timely installation of security updates reduces vulnerabilities that malware can exploit. The finding is in line with Nweke and Teixeira's (2023) systematic review reporting that patch management is a persistent challenge in government agencies.User awareness was significantly associated with effectiveness ($\beta = 0.198$, $p = 0.009$). This confirms GDT, according to which awareness of security policies and their consequences can lead to policy compliance. However, the weaker coefficient compared to training shows that only awareness is not enough – the practical skills and training are required.

Resource allocation ($\beta = 0.146$, $p = 0.042$) and technology type ($\beta = 0.142$, $p = 0.047$) were significant, but weaker predictors. This contradicts the assumption that acquisition of advanced technology can solve cybersecurity problems of the organization. Rather, technology, people's skills, and organizational practices contribute to outcomes. Policy enforcement was not statistically significant at the 5% level ($\beta = 0.128$, $p = 0.064$). This does not mean that the policy enforcement is ineffective; however, there was not enough evidence to make a conclusion about the significance of the correlation. Only 30.9% of respondents were aware of the security policies, and this can limit the influence of the policies. According to GDT, the policy enforcement is possible only when the policies are known and consistently applied. Because of the cross-sectional design, the findings demonstrate the existence of correlations rather than causations. Additionally, the lack of economic cost data precludes conclusions about financial returns on security investment.

Comparison with Related Literature

Internationally, the findings confirm the observations made by Al-Duwairi and Al-Eroud (2021) concerning the development of malware threats and the limitations of signature-based detection technologies. The low percentage of zero-day detections is in agreement with the findings of Patel and Soni (2022) about the limitations of signature-based solutions. The fact that only 34% of government organizations adopted behaviour-based or AI-driven solutions reported by Smith and Perez (2021) shows the prevalence of traditional solutions in Homa Bay County.

In Africa, the findings corroborate Chukwuma's (2022) assessment of resource constraints, skill gaps, and infrastructure weaknesses as major cybersecurity issues of public-sector organizations. They also confirm Adeyemi's (2022) finding that the African public-sector organizations mostly use signature-based technologies and disable some of the advanced options of the solutions because of performance issues. In the current study, heuristics was disabled on three systems due to concerns about false-positive detection.

Within Kenya, the findings corroborate Wanjiku's (2023) and Njenga's (2023) observations about configuration gaps and inconsistency of the update practices. The strong association between patch management and effectiveness highlights the importance of automation of updates and centralized security management.

The study expands the existing literature by quantitatively assessing the importance of the factors that affect the effectiveness of anti-malware technologies and comparing user perceptions with technical findings. Moreover, the study provided technical evidence which can complement self-reported data. Non-significant

association with policy enforcement reveals the necessity of policies to be known, understood and consistently enforced in order to become deterrent.

Recent evidence. The findings support recent evidence that unpatched vulnerabilities (not malware detection) drive compromise: Verizon's (2025) analysis of 12,195 confirmed breaches found vulnerability exploitation to be the initial access vector in 20% of breaches (up 34% year on year), supporting patch management strength as predictor here ($\beta = 0.312$) and gap in third-party patching (66.7%). In Kenya CA reported 4.56 billion cyber-threat events Oct–Dec 2025 and blamed weak patching, low user awareness of phishing and criminals' use of AI for rise (AllAfrica, 2026); these are not breaches but pattern matches two phishing repeat infections here and place of training as strongest predictor. OS lifecycle too matters. Windows 10 support ended on 14 October 2025 and extended support for Windows Server 2016 ends on 12 January 2027 (Microsoft, 2025).

Ten of the 12 audited systems ran Windows 10 Pro and one server ran Windows Server 2016 (Table 4.6) so the 83.3% "fully updated" rate recorded in April–May 2025 no longer provides protection because unsupported systems cannot be patched. NIST SP 800-40 Rev. 4 (Souppaya & Scarfone, 2022) treats patching as planned preventive maintenance with defined maintenance windows fits the delayed server updates and supports compensating controls where patching has to wait.

Explanation of Unexpected Findings

Unexpectedly, non-IT users expressed confidence in the effectiveness of anti-malware technologies despite serious technical gaps. Users may believe that any visible security feature implies protection, may have little experience of dealing with advanced malware, or may lack the technical knowledge that is required to understand the real capabilities of security software. As a result, awareness programmes should provide a clear understanding of the capabilities and limitations of security technologies.

Unexpectedly, the association between technology type and effectiveness appeared to be weaker compared to training and patch management. The finding shows that, in resource-constrained environments, improvement of configuration, updates, and development of people's skills may be more important than purchase of advanced technologies. Nevertheless, the limited capability to detect zero-day threats remains a serious problem.

Implications of the Findings.

Theoretical Implications.

The study expands TAM by the suggestion that perceived usefulness in the mandatory-use environment may be based on visible but limited information and requires technical validation. The association between training and effectiveness supports the PMT that emphasizes the importance of coping appraisal, while the findings regarding the policy enforcement reveal that GDT's deterrent effects depend on consistent policies enforcement.

Practical Implications

Homa Bay County should address the configuration weaknesses before implementing new technologies. The priorities include enabling of scheduled scans, automation of updates, improving server protection, and conducting third-party application patching. The standardization of products and introduction of centralized management will facilitate monitoring and coordination. Behaviour-based detection and endpoint detection and response solutions should be considered as resources become available. Training should remain a key element of the anti-malware programme.

Policy Implications

At county level, the findings suggest the establishment of standard configuration baselines, centralized patch

management and regular technical audits. At national level, the Ministry of ICT and the Communications Authority of Kenya should set baseline cybersecurity standards for county governments and give technical guidelines on selection and configuration of endpoint protection.

Implications for Future Research

Future research should include independent benchmarking of anti-malware products in African public-sector environment, multi-county comparison, longitudinal investigation of improvements of configuration and patching, and cost-effectiveness assessment of cybersecurity investments.

Summary

The anti-malware technologies of Homa Bay County Government provide baseline protection against known threats, but are constrained by configuration weaknesses, uneven patching, non-standardized products, and the lack of zero-day detection. Users' confidence may exceed the technical evidence. Training and patch management are the factors most strongly associated with effectiveness, which implies that cybersecurity is as dependent on people and discipline as on technologies.

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Introduction

This chapter summarizes the study's findings, draws conclusions, gives recommendations for practice and policy, highlights limitations of the study and identifies directions for future research.

Summary of the Study

The study evaluated the effectiveness of anti-malware technologies implemented in Homa Bay County Government using the mixed-methods case study design. Data were collected using a structured questionnaire completed by 136 respondents (response rate 90.7%), semi-structured interviews with four ICT key informants, and technical audit of 12 systems. The questionnaire data were analysed using descriptive statistics and multiple regression; the interview and audit findings were analysed thematically and descriptively.

Summary of Key Findings

Technologies Deployed and Their Performance

It was found that the County Government had deployed near-universal endpoint protection, but the technologies were not standardized. Windows Defender for Endpoint was mentioned by 62.1% of respondents, and Kaspersky Endpoint Security was mentioned by 41.4%. Malwarebytes, Symantec, and Avant were also used on limited number of systems. The lack of standardization complicates the monitoring, coordination of updates, and security management.

Technical audit revealed that all 12 systems had real-time protection. Automatic definition updates were enabled on 10 systems (83.3%), and two servers had manually performed weekly updates because of the possibility of service interruption. Scheduled scans were configured on eight systems (66.7%), leaving four workstations without them. Heuristic or behaviour-based detection was used on nine systems (75%), and cloud threat intelligence was available on 10 systems (83.3%).

During the 12-month audit period, 42 malware detections were recorded. The internal logs indicated the detection rate of 95%, while 88% were detected using the independent tools. Therefore, some threats may bypass the primary anti-malware technology. Only three detections (about 7%) were classified as zero-day threats, implying the limited capability of detecting the previously unknown malware.

Although 82.4% of respondents rated the effectiveness as moderate or high and 57.4% were satisfied with the system performance, there were some weaknesses in zero-day detection, scheduled scans, and third-party patching. The differences indicate that visible alerts and automatic cleaning may influence user's confidence in security but does not demonstrate the protection from advanced attacks.

ICT Department had the incident response plan which was last updated 10 months ago and the response team consisted of Head of ICT, System Administrator, and Network Security Officer. The average response time to the identified threats was two hours, and the incident documentation provided the basis for containment, eradication, and recovery activities.

Updates of operating systems were available on 10 systems (83.3%), and two servers had delayed updates due to the stability testing. There was weaker third-party application patching with only eight systems (66.7%) having all critical applications, including browsers, PDF readers, and office suites, patched.

Summary of Regression Analysis Findings

The regression model explained 61.2% of the variance in anti-malware effectiveness ($R^2 = 0.612$). Training was the strongest predictor ($\beta = 0.356$, $p < 0.001$), followed by patch management ($\beta = 0.312$, $p < 0.001$). User awareness was significant ($\beta = 0.198$, $p = 0.009$), while resource allocation ($\beta = 0.146$, $p = 0.042$) and technology type ($\beta = 0.142$, $p = 0.047$) had weaker but statistically significant associations.

Policy enforcement was not statistically significant at the 5% level ($\beta = 0.128$, $p = 0.064$). The limited policy awareness may limit the influence of formal security rules. Overall, the findings show that anti-malware effectiveness is associated with human, technical, and organizational factors, corroborating the theoretical framework of PMT, GDT, and TAM.

The regression equation was: Effectiveness = 1.234 + 0.412 (Training) + 0.378 (Patch Management) + 0.156 (Technology Type) + 0.224 (User Awareness) + 0.142 (Policy) + 0.168 (Resources).
Such results indicate associations but not causations.

Conclusions

The study has six main conclusions.

First, the County has established baseline protection with wide spread installation of anti-malware software and real-time protection. However, weaknesses in automatic updates, scheduled scans, and third-party patching expose the systems to avoidable risks. Second, the County has limited capability to detect zero-day and other advanced threats. The prevalence of signature-based detection technologies makes it impossible to detect novel, polymorphic, and fileless malware. The behaviour-based detection, heuristic analysis, and improved threat intelligence should be considered.

Third, the usage of multiple anti-malware products complicates management, monitoring, configuration, and policy enforcement. The standardization and centralized management should be considered. Fourth, patch management is still a significant issue, especially in third-party applications. While updates of operating systems are relatively common, the incomplete patching of browsers, PDF readers, and office suites leaves the exploitable vulnerabilities.

Fifth, the effectiveness is more strongly associated with staff training and patch management than with the technology type. The County should combine the investment in security tools and the development of people's skills and discipline. Sixth, users' confidence exceeds technical evidence. Effectiveness was rated moderate or high by 82.4% but only 57.4% were satisfied and four of 12 systems had scheduled scans not performed; only 66.7% third-party patching completed; only 3 of 42 detections zero-day. Awareness programmes need to explain what the tools can and cannot do.

Recommendations

Recommendations for Homa Bay County Government
Standardize and centralize anti-malware protection. Consolidate the endpoint protection on one platform with a central management console for unified policies, updates, scans, and alerts. It will take 6–12 months after budget allocation and procurement.

Automate patch management. Implement automated patching of operating systems and third-party applications, establish the agreed-upon update windows, and prepare monthly patch-compliance reports. It will take six months.

Implement scheduled scans. Start performing weekly quick scans and monthly full scans on all systems, preferable outside of the peak operating hours. It will take one month.

Improve server protection. Where automatic updates are delayed for the stability reasons, test patches on non-critical systems first and implement compensating controls, such as application allow-listing, enhanced monitoring, network segmentation, and host-based intrusion detection. It will take three to six months.

Activate behaviour-based detection. Turn on and properly configure heuristic detection, manage false positives, and consider the endpoint detection and response or managed detection services where the resources allow.

Improve vulnerability assessments and incident response. Perform monthly vulnerability scans of critical systems, assign the responsibility for remediation, and review and test the incident response plan at least every six months.

Invest in staff training. Train ICT staff in endpoint security and educate all employees on safe computing, security procedures, and the capabilities and limitations of anti-malware technologies.

Recommendations for National Government and Regulators

The Ministry of ICT and the Communications Authority of Kenya should develop minimum cybersecurity standards for county governments, including the configuration and patching requirements. They should also provide technical assistance, consider the shared services (e.g., the common security operations centre) and examine possibilities for dedicated funding for cybersecurity of county governments.

The study concentrated on one county government; therefore, its findings cannot be statistically generalized to all counties. The technical audit included only 12 purposively selected systems, and the detection rates were calculated based on system logs and limited independent scanning, not on the product testing. The effectiveness scores were partially based on user perceptions that may differ from technical performance. The cross-sectional design made it possible to reveal the correlations but not causations, while the lack of cost data precluded the conclusions about financial returns on investment.

Limitations of the Study

Recommendations for Further Research

Further research should be focused on:

Independent technical benchmarking of anti-malware products in African public-sector environment.

Comparison of configuration, patching, and detection performance in several counties.

Longitudinal and intervention studies of the impact of staff training and patch management.

Economic evaluation of cost-effectiveness of cybersecurity investments in county governments.

Contribution to Theory and Practice

The study expanded TAM by showing that perceived usefulness in the mandatory-use environment may differ from technical reality. It facilitates PMT in the importance of training and shows when GDT's hypotheses about policy deterrence could be accurate. The practical benefits include the identification of configuration and patching vulnerabilities that could be mitigated with current capabilities and areas that require additional resources. The methodological contributions include the use of the combination of user perception with technical audits and an audit technique that could be used by other counties.

Final Conclusion

Anti-malware systems in the Homa Bay County Government have a working and required layer of protection but offer a moderate level of effectiveness. This is determined by configuration and patching vulnerabilities, product fragmentation, and poor detection capabilities for emerging threats. There is likely to be more trust in the protection capabilities than is justified based on technical data. The County could increase the effectiveness of its solutions through the standardization and centralization of its anti-malware products, improved discipline in configuration and patching, and additional training of employees. Later, advanced detection systems could be acquired when the situation allows. Proper cybersecurity needs a balanced combination of technology, personnel skills, and good management practices.

REFERENCES

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 behavior 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-behavioral 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. Nweke, L. O., & Teixeira, T. (2023). Challenges and opportunities in cybersecurity for government organizations. Journal of Cyber Policy, 8(2), 204-222.
51. 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.
52. 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.
53. 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.
54. 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.
55. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.
56. 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.
57. 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.
58. 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.
59. Serianu. (2023). Africa cybersecurity report: Kenya country report. Serianu Limited.
60. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.
61. Smith, J., & Perez, A. (2021). Evaluating anti-malware technologies in modern information systems. International Journal of Cybersecurity Research, 18(2), 145-160.
62. 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.
63. 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.
64. Thompson, S. K. (2012). Sampling (3rd ed.). John Wiley & Sons.

65. 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.
66. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204.
67. 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.
68. Wanjiku, M. (2023). Malware threats and cybersecurity measures in Kenyan county governments. Kenya Journal of Information Systems, 5(1), 78-92.
69. World Economic Forum. (2024). The Global Risks Report 2024 (19th ed.). World Economic Forum.
70. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.