International Research Journal of Rongo University (IJORU) ISSN: 3005-7221
Transformative Research and Innovation for an Inclusive and Sustainable Future
Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

CYBERSECURITY PREPAREDNESS IN COUNTY E-GOVERNMENT SYSTEMS: A CASE STUDY OF BOMET COUNTY, KENYA

[1]Felody Chepkirui*, [1]James Abila, [1]Lamek Ronoh

*Corresponding Author: felodychepkirui96@gmail.com

https://orcid.org/0009-0005-0980-2207; https://orcid.org/0000-0003-0805-214X; https://orcid.org/0000-0003-0385-280X;

[1]Rongo University, P.O. Box 103-40404 Rongo, Kenya

Abstract

Kenya's adoption of e-government systems has significantly improved public service delivery, transparency, and citizen participation within county governments. However, the increasing reliance on digital technologies has also heightened exposure to cybersecurity threats, including phishing, ransomware, unauthorized access, and data breaches. Although national frameworks such as the Data Protection Act (2019) and the National Cybersecurity Strategy (2022–2027) provide guidance for securing digital systems, empirical evidence on cybersecurity preparedness within county governments remains limited. Existing studies have largely focused on national government institutions, leaving a knowledge gap regarding the preparedness of devolved governments to secure their e-government systems. This study therefore evaluated the level of cybersecurity preparedness in Bomet County's e-government systems by examining technical controls, policy implementation, and human capacity. The broader study adopted a Design Science Research (DSR) framework, while this paper presents findings from the mixed-methods assessment undertaken to address the first study objective. Quantitative data were collected using structured questionnaires administered to county employees and ICT personnel (n = 45), while qualitative data were obtained through semi-structured interviews with key informants. Quantitative data were analyzed using descriptive statistics, while qualitative data were analyzed thematically to provide contextual insights into cybersecurity practices and challenges. The findings indicate that cybersecurity preparedness in Bomet County is moderate despite the presence of basic security controls. Approximately 66.7% of respondents had not received formal cybersecurity training during the previous twelve months, while 55% reported experiencing cybersecurity incidents, highlighting significant gaps in staff capacity, policy implementation, and incident response. Although access control mechanisms were available, their effectiveness was constrained by inadequate cybersecurity awareness and weak policy enforcement. The study concludes that strengthening staff capacity, improving policy implementation, and institutionalizing regular cybersecurity preparedness assessments are essential for enhancing the resilience of county e-government systems. The findings provide empirical evidence to support county-level cybersecurity governance and offer practical insights for strengthening secure and sustainable digital service delivery within devolved government institutions.

Keywords: *Cybersecurity preparedness, e-government, county governments, digital governance, cybersecurity governance, Kenya*.

Introduction

The rapid digital transformation of public administration has positioned e-government systems as a cornerstone of modern governance by enhancing service efficiency, transparency, accountability, and citizen participation. In Kenya, the implementation of the devolved system of government has accelerated the adoption of digital technologies across county governments, with

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

information systems increasingly supporting critical functions such as revenue administration, financial management, health information systems, and citizen service delivery. While these digital initiatives have improved administrative efficiency and accessibility of public services, they have simultaneously expanded the cyber threat landscape, exposing county information systems to phishing attacks, ransomware, malware, unauthorized access, data breaches, and service disruptions. Consequently, cybersecurity preparedness has become an essential prerequisite for safeguarding the confidentiality, integrity, and availability of digital government services. Kenya has responded by establishing legal and policy frameworks, including the Data Protection Act (2019) and the National Cybersecurity Strategy (2022–2027), to strengthen national cybersecurity governance. Nevertheless, there is limited empirical evidence demonstrating the extent to which these frameworks have been implemented within county governments and their contribution to organizational cybersecurity preparedness.

Contemporary cybersecurity literature increasingly recognizes preparedness as a multidimensional organizational capability rather than merely the implementation of technical safeguards. Effective cybersecurity preparedness requires the integration of technological controls, institutional governance, risk management processes, and human capacity to enable organizations to anticipate, prevent, detect, respond to, and recover from cyber threats. The European Union Agency for Cybersecurity (ENISA, 2023) identifies continuous risk assessment, monitoring, and incident response as critical elements of organizational resilience, while the National Institute of Standards and Technology (NIST, 2018) Cybersecurity Framework and ISO/IEC 27005 advocate a risk-based approach to cybersecurity management through continual assessment and improvement of security controls. Recent empirical studies further demonstrate that local government cybersecurity preparedness depends on coordinated governance structures, workforce competence, organizational policies, and technical safeguards rather than technology alone (Hossain et al., 2024; Norris et al., 2024). Similarly, Gupta et al. (2021) observed that inconsistent policy implementation and weak governance structures substantially undermine the effectiveness of technical security controls. Collectively, these studies reinforce the view that cybersecurity preparedness should be understood as a socio-technical phenomenon requiring coordinated investment in people, processes, governance, and technology.

Despite growing recognition of cybersecurity as a strategic governance issue, achieving effective cybersecurity preparedness remains particularly challenging for local governments in developing countries. Resource limitations, inadequate cybersecurity expertise, inconsistent policy implementation, insufficient workforce training, and weak incident response capabilities continue to constrain organizational resilience. These challenges are especially evident within Kenya's devolved governance system, where the rapid expansion of e-government services has not always been accompanied by proportional investments in cybersecurity capacity. Consequently, many county governments continue to rely on reactive cybersecurity practices, increasing their exposure to evolving cyber threats and reducing the resilience of digital public services. Similar challenges have been reported across developing countries, where fragmented governance structures, limited institutional capacity, and resource constraints continue to hinder effective cybersecurity implementation within local government institutions (Hossain et al., 2024; Mushtaq & Shah, 2024).

Although cybersecurity has attracted increasing scholarly attention, much of the existing research has focused on national governments, private-sector organizations, or general public-sector institutions. Comparatively fewer empirical studies have examined cybersecurity

preparedness within county or local government environments, whose governance arrangements, operational responsibilities, and institutional constraints differ considerably from those of national government agencies. Furthermore, existing studies have rarely examined cybersecurity preparedness by simultaneously considering the interaction between technical controls, organizational governance, and human capacity within devolved e-government environments. Recent reviews similarly conclude that empirical evidence on cybersecurity preparedness within local governments remains limited, particularly in developing countries where contextual factors substantially influence cybersecurity outcomes (Hossain et al., 2024). This knowledge gap limits the availability of context-specific evidence needed to support cybersecurity policy development, resource allocation, organizational capacity building, and evidence-based decision-making at the county government level. Addressing this gap is particularly important because county governments increasingly depend on interconnected digital systems to deliver essential public services and manage sensitive citizen information.

This study is grounded in the Socio-Technical Systems Theory, which argues that organizational performance emerges from the interaction between technological systems, organizational structures, and human behavior. Within the cybersecurity context, the theory suggests that organizational preparedness cannot be achieved solely through the implementation of technical controls but requires the alignment of governance mechanisms, institutional policies, employee capabilities, and organizational practices. The broader study adopted a Design Science Research (DSR) framework to investigate cybersecurity challenges within county e-government systems and ultimately develop a context-specific cybersecurity risk assessment model. However, the present paper reports findings relating only to the first phase of the broader study, which evaluates cybersecurity preparedness within Bomet County's e-government systems. Accordingly, cybersecurity preparedness is conceptualized through three interrelated dimensions: technical controls, organizational governance, and human capacity which collectively determine the ability of county governments to anticipate, prevent, detect, respond to, and recover from cybersecurity threats.

This study evaluated the level of cybersecurity preparedness within Bomet County's e-government systems by examining the implementation of technical controls, organizational governance practices, and human capacity. Specifically, the study sought to answer the following research question:

What is the level of cybersecurity preparedness in Bomet County's e-government systems?

The findings contribute empirical evidence to the limited body of knowledge on cybersecurity preparedness within Kenya's devolved governments and provide practical insights for strengthening cybersecurity governance, institutional capacity, policy implementation, and risk management. The study further contributes to the growing discourse on cybersecurity preparedness in local government settings by providing context-specific evidence that can inform secure, resilient, and sustainable digital public service delivery in Kenya and other developing countries.

Research Methodology

This study forms part of a broader investigation that adopted the Design Science Research (DSR) methodology to examine cybersecurity challenges within county e-government systems and support the development of a context-specific cybersecurity risk assessment model. While the broader study involved multiple phases culminating in the design of the proposed model, this paper reports findings from the first phase, which focused on evaluating cybersecurity preparedness in Bomet County's e-government systems. A mixed-methods research design was adopted to

integrate quantitative and qualitative evidence, thereby providing a comprehensive assessment of cybersecurity preparedness. Quantitative data were used to assess cybersecurity awareness, existing security practices, and the implementation of cybersecurity controls, whereas qualitative data provided contextual insights into organizational experiences, governance practices, and challenges affecting cybersecurity preparedness. Integrating both approaches enhanced methodological triangulation and strengthened the credibility of the findings (Creswell & Plano Clark, 2018).

The study was conducted within the County Government of Bomet, targeting employees involved in the use, administration, and management of county e-government systems, including ICT personnel, system administrators, and users from departments that routinely interact with digital information systems. The target population comprised approximately 70 respondents, identified from departmental records. Sample size determination was guided by the Krejcie and Morgan (1970) sample size determination table, which recommended a sample of 60 respondents for the target population. Owing to accessibility constraints and response rates, 45 completed questionnaires were successfully collected and analyzed. In addition, three key informants responsible for ICT management and cybersecurity oversight participated in semi-structured interviews, providing complementary qualitative evidence.

A purposive stratified sampling technique was employed to ensure that respondents possessed relevant knowledge and practical experience relating to county e-government systems. Departments were treated as strata to achieve representation from both technical and non-technical functional areas, including ICT, Finance, Health, Administration, and other operational departments. Purposive selection within each stratum facilitated the inclusion of respondents directly involved in the implementation, management, or use of county information systems, thereby providing comprehensive insights into cybersecurity preparedness across the county government.

Data were collected using three complementary approaches. First, a structured questionnaire was administered to county employees to obtain quantitative data on cybersecurity awareness, staff training, policy implementation, security practices, and perceptions of cybersecurity preparedness. The questionnaire was developed following a review of established cybersecurity frameworks, including the NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27005:2022, together with relevant literature on cybersecurity preparedness. The instrument was subsequently refined through expert review to ensure its suitability for the county government context. Second, semi-structured interviews were conducted with three key informants to obtain detailed information regarding organizational governance, policy implementation, institutional capacity, and cybersecurity challenges that could not be adequately captured through structured questionnaires. Combining questionnaires and interviews strengthened methodological triangulation by integrating measurable indicators with contextual explanations.

To complement the self-reported data, a non-intrusive technical assessment of selected county e-government systems was undertaken. Unlike penetration testing, the assessment did not involve active exploitation or unauthorized access to operational systems. Instead, it focused on reviewing system configurations, observing existing security practices, evaluating access control mechanisms, assessing patch management processes, identifying common vulnerabilities, and examining available documentation relating to cybersecurity controls. This approach provided an independent assessment of the county's cybersecurity posture while ensuring that normal government operations remained

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

uninterrupted and that ethical requirements governing public-sector information systems were fully observed.

The validity of the research instruments was established through expert review, during which the questionnaire and interview guide were evaluated for clarity, relevance, and alignment with the study objectives prior to data collection. Instrument reliability was assessed through a pilot study, with internal consistency evaluated using Cronbach's alpha coefficient. All constructs recorded Cronbach's alpha values exceeding the generally accepted threshold of 0.70, indicating acceptable internal consistency and satisfactory reliability of the study instruments (Taber, 2018).

Quantitative data were analyzed using IBM SPSS Statistics Version 25. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize respondents' demographic characteristics, cybersecurity awareness, training, policy implementation, and preparedness indicators. In addition, Pearson correlation analysis was conducted to examine the relationships between selected organizational factors and cybersecurity preparedness. Qualitative data obtained from interviews were analyzed thematically through coding, categorization, and identification of recurring themes relating to cybersecurity governance, organizational practices, technical challenges, and institutional capacity. Findings from the questionnaires, interviews, and technical assessment were subsequently triangulated to enhance the validity, consistency, and credibility of the overall findings by allowing evidence generated through one method to corroborate evidence obtained from the others.

Ethical approval for the study was obtained through the relevant institutional and county authorization processes before data collection commenced. Participation was voluntary, and informed consent was obtained from all respondents. Confidentiality and anonymity were maintained throughout the study, while all collected data were handled in accordance with applicable data protection requirements. Furthermore, the non-intrusive technical assessment was conducted without disrupting county information systems and did not involve unauthorized access, modification, or interference with operational digital infrastructure.

Results

This section presents the findings of the study on cybersecurity preparedness within Bomet County's e-government systems. The results are organized into six thematic areas: respondent characteristics, cybersecurity awareness, cybersecurity capacity and practices, implementation of cybersecurity controls, cybersecurity incident experience, Pearson correlation analysis, and a summary of the key findings.

Respondent Characteristics

A total of 45 respondents completed the questionnaire survey. Participants were drawn from the ICT, Finance, Administration, Health, and other county departments to ensure representation from both technical and non-technical personnel involved in the operation, management, and use of the county's e-government systems. The ICT department contributed the highest proportion of respondents (51.1%), followed by Finance, Administration, Health, and other operational departments.

The demographic profile indicates that most respondents were aged between 26 and 45 years, with the majority having one to three years of service within the county government. This distribution provided perspectives from employees who were actively engaged in the day-to-day use and management of county information systems, making them well positioned to provide informed views on cybersecurity preparedness.

International Research Journal of Rongo University (IJORU) ISSN: 3005-7221
Transformative Research and Innovation for an Inclusive and Sustainable Future
Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

Figure 1
Departmental Distribution of Respondents

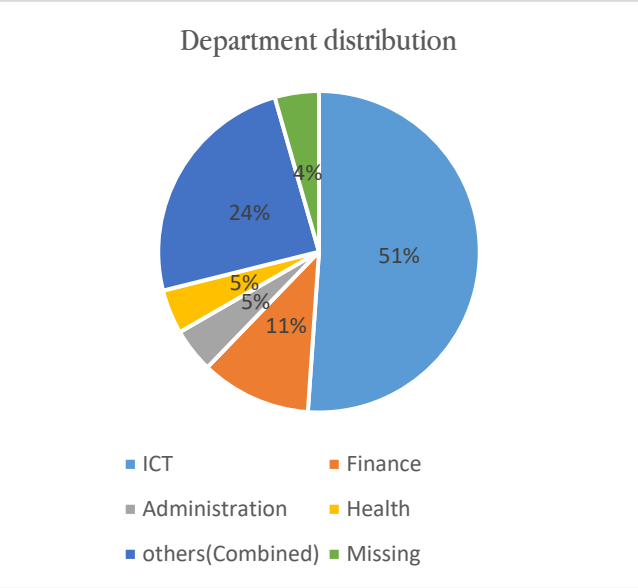
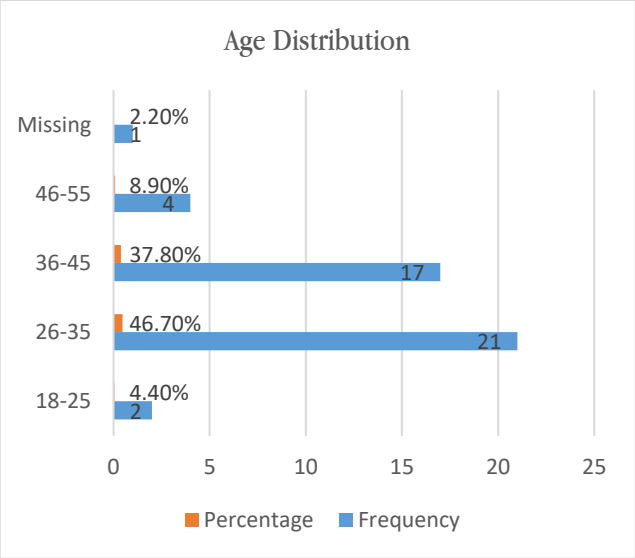


Figure 2
Age Distribution of Respondents



Cybersecurity Awareness

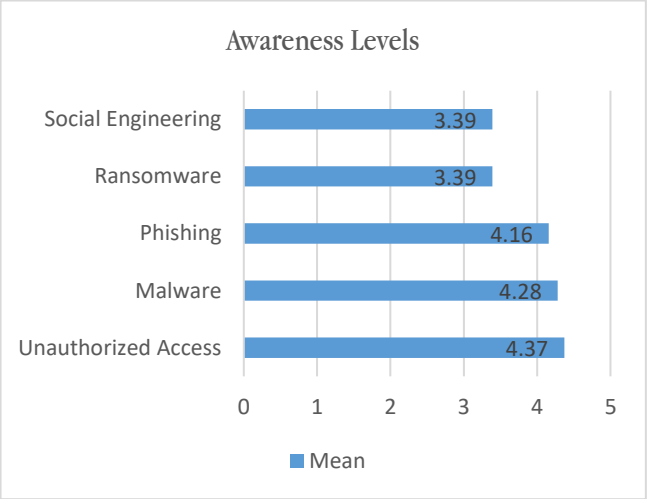
Respondents were asked to evaluate their level of awareness of selected cybersecurity threats relevant to county e-government systems. The findings indicate an overall mean awareness score of 3.94, reflecting a moderate-to-high level of cybersecurity awareness among the respondents.

Awareness was greatest for unauthorized access (M = 4.37), malware (M = 4.28), and phishing attacks (M = 4.16). In comparison, respondents reported relatively lower levels of awareness of ransomware (M = 3.39) and social engineering attacks (M = 3.39).

Table 1
Cybersecurity Awareness Levels

Threat	Mean	Interpretation
Unauthorized Access	4.37	High
Malware	4.28	High
Phishing	4.16	High
Ransomware	3.39	Moderate
Social Engineering	3.39	Moderate

Figure 3
Mean Cybersecurity Awareness Levels



Cybersecurity Capacity and Practices

The findings indicate limited investment in cybersecurity capacity development among county employees. Approximately 66.7% of respondents reported that they had not received formal cybersecurity training during the preceding twelve months, whereas only 33.3% indicated that they had participated in such training.

A similar pattern was observed with respect to cybersecurity awareness programs. Most respondents (62.2%) indicated that awareness programs were conducted rarely, while comparatively fewer

respondents reported that such programs were implemented annually or more frequently.

The qualitative findings corroborated these results. Interview participants consistently identified inadequate staff training and the limited implementation of continuous cybersecurity awareness programs as key challenges affecting cybersecurity preparedness within the county.

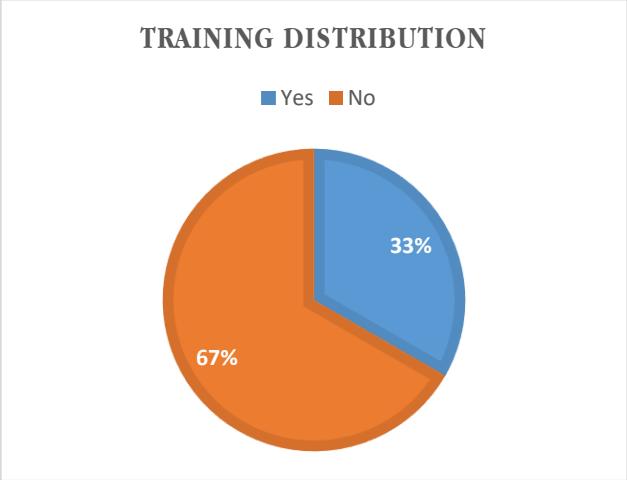
Table 2

Cybersecurity Training Participation

Category	Percentage (%)
Received Training	33.3
No Training	66.7

Figure 4

Cybersecurity Training Participation



Implementation of Cybersecurity Controls

The level of implementation of cybersecurity controls varied across the assessed control areas. Access control mechanisms emerged as the most widely implemented security measure, with 91.1% of respondents indicating that county information systems restricted access to authorized users. Similarly, 71.1% of respondents confirmed that routine data backup procedures were implemented to support information security and system recovery.

Moderate levels of implementation were observed for patch management and policy adherence. In contrast, fewer respondents (37.8%) reported the existence of formal incident reporting procedures, while only 15.6% indicated that regular cybersecurity risk assessments were conducted within the county.

The qualitative findings reinforced these observations. Interview participants reported inconsistent enforcement of cybersecurity policies and identified weaknesses in incident reporting procedures across county departments.

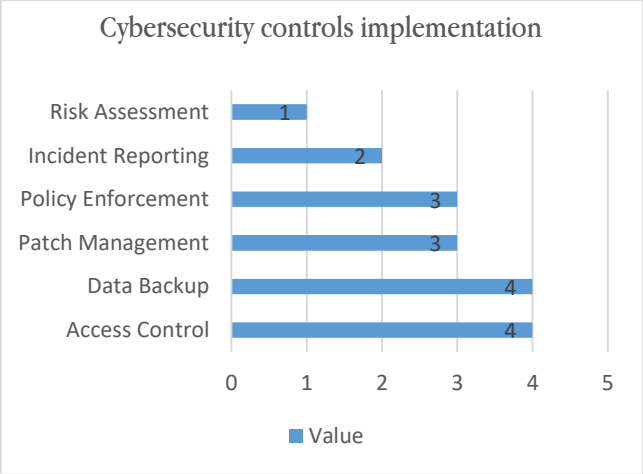
Table 3

Implementation of Cybersecurity Controls

Control Area	Level of Implementation
Access Control	Strong
Data Backup	Strong
Patch Management	Moderate
Policy Adherence	Moderate
Incident Reporting	Weak
Regular Risk Assessment	Very Weak

Figure 5

Implementation of Cybersecurity Controls



Cybersecurity Incident Experience

More than half of the respondents (55%) reported having experienced at least one cybersecurity incident while using the county's e-government systems.

Among the reported incidents, system downtime was the most common (45%), followed by unauthorized access (30%) and data loss (25%). Malware accounted for 22.5%

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

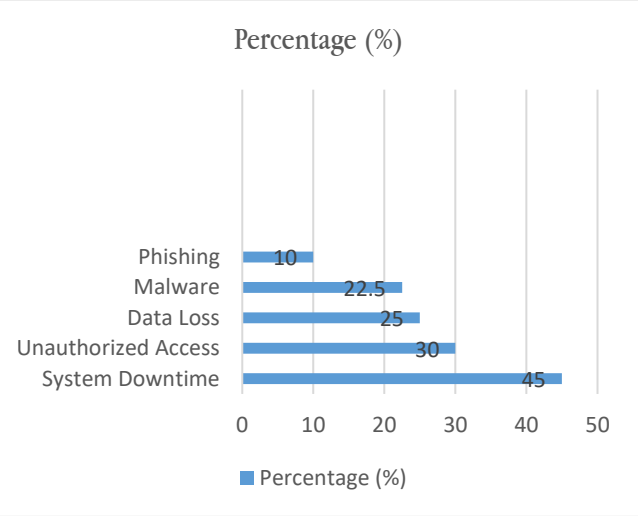
of the reported incidents, whereas phishing attacks were the least frequently reported (10%).

The qualitative findings were consistent with the survey results. Interview participants identified system downtime, delayed incident reporting, and unauthorized system access as recurring cybersecurity challenges affecting county operations.

Table 4
Reported Cybersecurity Incidents

Incident Type	Percentage (%)
System Downtime	45.0
Unauthorized Access	30.0
Data Loss	25.0
Malware	22.5
Phishing	10.0

Figure 6
Distribution of Cybersecurity Incidents



Pearson Correlation Analysis

Pearson correlation analysis was conducted to examine the relationships between cybersecurity preparedness and selected organizational factors.

The analysis revealed a statistically significant positive correlation between cybersecurity awareness and cybersecurity preparedness, $r = .317$, $p = .026$. Significant positive correlations were also observed between cybersecurity preparedness and confidence in county cybersecurity systems ($r = .717$, $p < .001$), policy adherence ($r = .809$, $p < .001$), and the frequency of cybersecurity awareness programs ($r = .757$, $p < .001$).

Table 5
Pearson Correlation between Cybersecurity Preparedness and Selected Variables

Variable	Pearson's r	p-value	Strength of Relationship
Cybersecurity Awareness	0.317	0.026	Weak Positive
Confidence in County Cybersecurity Systems	0.717	<0.001	Strong Positive
Policy Adherence	0.809	<0.001	Very Strong Positive
Frequency of Awareness Programs	0.757	<0.001	Strong Positive

All four variables demonstrated statistically significant positive relationships with cybersecurity preparedness.

Summary of Findings

The findings indicate a moderate-to-high level of cybersecurity awareness among respondents, although awareness of ransomware and social engineering attacks was comparatively lower than for other cybersecurity threats. The results also revealed limited investment in cybersecurity capacity development, with most respondents reporting that they had not received formal cybersecurity training during the preceding year and that cybersecurity awareness programs were implemented infrequently.

With respect to cybersecurity controls, access control and routine data backup were the most consistently implemented measures, whereas formal incident reporting procedures and regular cybersecurity risk assessments were less widely implemented. More than half of the respondents reported having experienced at least one cybersecurity incident, with system downtime and unauthorized access emerging as the most commonly reported incidents. Furthermore, the Pearson

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

correlation analysis identified statistically significant positive correlations between cybersecurity preparedness and cybersecurity awareness, confidence in county cybersecurity systems, policy adherence, and the frequency of cybersecurity awareness programs.

Discussion

This study examined cybersecurity preparedness within Bomet County's e-government systems by assessing cybersecurity awareness, capacity development, implementation of cybersecurity controls, cybersecurity incident experience, and the organizational factors associated with preparedness. The findings demonstrate that cybersecurity preparedness is shaped by the combined influence of human, organizational, and technical dimensions. This observation supports the socio-technical perspective adopted in this study, which recognizes that effective cybersecurity depends not only on technological safeguards but also on organizational practices and user behavior. The findings further align with established cybersecurity governance frameworks that advocate a balanced approach integrating people, processes, and technology (NIST, 2018; ISO/IEC 27001:2022).

Cybersecurity Awareness and Preparedness

The study found that respondents demonstrated a moderate-to-high level of cybersecurity awareness. Awareness was highest for commonly encountered threats, including unauthorized access, malware, and phishing attacks, whereas comparatively lower awareness was reported for ransomware and social engineering attacks. These findings suggest that employees are generally familiar with conventional cyber threats encountered during routine system use but may be less prepared to recognize increasingly sophisticated attacks that exploit human behavior.

The relatively lower awareness of ransomware and social engineering is noteworthy given the increasing prevalence of these attack vectors in public-sector environments. Unlike conventional malware, social engineering attacks primarily manipulate users through deception, while ransomware combines technical compromise with operational disruption, making both threats particularly challenging for organizations that depend heavily on digital service delivery. Consequently, strengthening employee awareness of emerging attack techniques is essential for improving organizational resilience.

These findings are consistent with recent studies highlighting cybersecurity awareness as a fundamental component of organizational preparedness. For example, Mushtaq and Shah (2024) reported that employee awareness significantly influences organizations' ability to prevent and respond to cyber threats, particularly within public institutions undergoing digital transformation. Similarly, Hossain et al. (2024) observed that awareness programs focusing on evolving attack techniques substantially improve employees' ability to identify phishing and social engineering attempts. Although the findings indicate a relatively satisfactory level of awareness of conventional threats, the lower awareness of ransomware and social engineering suggests that existing awareness initiatives should be broadened to address emerging cybersecurity risks.

The findings also reinforce the recommendations of the NIST Cybersecurity Framework, which identifies awareness and training as essential components of the Protect function (NIST, 2018). From a socio-technical perspective, strengthening cybersecurity awareness contributes not only to individual knowledge but also to the development of a security-conscious organizational culture capable of supporting secure digital service delivery.

Cybersecurity Capacity Development

The findings indicate that cybersecurity capacity development within Bomet County remains limited. Most respondents reported that they had not received

formal cybersecurity training during the preceding twelve months, while cybersecurity awareness programs were implemented infrequently. These findings suggest that although employees routinely interact with e-government systems, opportunities for continuous cybersecurity learning remain insufficient to keep pace with the evolving threat landscape.

From a socio-technical perspective, these findings highlight the importance of developing human capabilities alongside technological controls. Effective cybersecurity preparedness depends not only on the availability of technical safeguards but also on employees' knowledge, skills, and ability to apply secure practices in their daily responsibilities. Consequently, investments in cybersecurity technologies alone are unlikely to achieve sustainable organizational resilience without corresponding investments in workforce development.

The findings are consistent with recent empirical studies emphasizing continuous cybersecurity education as a critical determinant of organizational preparedness. Norris et al. (2024) found that organizations providing regular cybersecurity training reported higher levels of policy compliance, improved incident recognition, and stronger security cultures than organizations relying primarily on technical safeguards. Similarly, Prümmer et al. (2024) found that continuous cybersecurity training and awareness initiatives enhance employees' ability to recognize emerging cyber threats and respond more effectively to security incidents. These observations are particularly relevant to public-sector organizations, where financial constraints, competing institutional priorities, and limited cybersecurity expertise often constrain investment in workforce capacity development. Furthermore, van den Berg et al. (2025) demonstrated that sustained cybersecurity training contributes to a stronger organizational security culture and promotes secure employee behavior over time.

The positive association identified between the frequency of cybersecurity awareness programs and cybersecurity preparedness further reinforces the importance of continuous staff development. Regular awareness initiatives help strengthen secure workplace behaviors, improve compliance with organizational security policies, and promote a culture of shared responsibility for cybersecurity across government institutions. Accordingly, awareness programs should be integrated into routine organizational practice rather than being implemented solely to satisfy compliance requirements.

These findings are further supported by internationally recognized cybersecurity frameworks. Both the NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27001:2022 emphasize awareness, competence, and continuous improvement as essential components of an effective information security management system. Strengthening cybersecurity capacity through structured training, continuous awareness initiatives, and ongoing professional development is therefore likely to enhance the resilience of county e-government systems against increasingly sophisticated cyber threats.

Implementation of Cybersecurity Controls

The findings indicate that the implementation of cybersecurity controls within Bomet County's e-government systems is uneven. Although access control mechanisms and routine data backup practices were widely implemented, comparatively lower levels of implementation were observed for patch management, formal incident reporting procedures, policy adherence, and regular cybersecurity risk assessments. This pattern suggests that while the county has established essential technical safeguards, governance and operational processes required to support sustainable cybersecurity management remain insufficiently developed.

The widespread implementation of access control mechanisms reflects recognition of the need to restrict system access to authorized users, thereby protecting the

confidentiality and integrity of government information assets. Likewise, routine data backup contributes to organizational resilience by facilitating data recovery and supporting continuity of digital services following cybersecurity incidents. However, recent studies emphasize that technical controls alone cannot ensure effective cybersecurity without complementary governance structures and continuous risk management practices (Hossain et al., 2024).

The limited implementation of incident reporting procedures and routine cybersecurity risk assessments points to important organizational gaps. Structured incident reporting enables timely detection, documentation, and response to security events, while periodic risk assessments help organizations identify vulnerabilities, evaluate emerging threats, and prioritize mitigation measures. The absence of these governance-oriented practices suggests that cybersecurity management within the county remains more reactive than preventive. Similar findings were reported by Hossain et al. (2024), who observed that many local governments have invested in technical safeguards but continue to experience weaknesses in governance, policy implementation, and continuous cybersecurity monitoring.

The qualitative findings further support these observations. Interview participants described inconsistent enforcement of cybersecurity policies and limited coordination of incident response activities across county departments. These findings indicate that although cybersecurity policies may exist, their implementation is not consistently monitored or enforced, potentially reducing compliance and increasing organizational exposure to cyber threats.

From a theoretical perspective, these findings reinforce the socio-technical systems perspective, which views cybersecurity as the outcome of interactions among technology, organizational governance, and human behavior. The findings also align with the NIST Cybersecurity Framework, which identifies the Identify, Protect, Detect, and Respond functions as interconnected elements of effective cybersecurity governance (NIST, 2018). Similarly, ISO/IEC 27005:2022 emphasizes continuous risk assessment, monitoring, and risk treatment as integral components of information security risk management. Collectively, these findings suggest that strengthening governance processes, improving policy implementation, and institutionalizing continuous risk management would substantially enhance cybersecurity preparedness within county e-government systems.

Cybersecurity Incidents and Organizational Preparedness

The findings indicate that more than half of the respondents had experienced at least one cybersecurity incident while using the county's e-government systems. System downtime, unauthorized access, and data loss were the most frequently reported incidents, demonstrating that operational disruptions continue to affect the county's digital environment despite the implementation of basic cybersecurity controls. These findings suggest that effective cybersecurity preparedness extends beyond preventive technologies to include robust capabilities for incident detection, response, and recovery.

System downtime emerged as the most commonly reported incident, highlighting its potential implications for the availability and continuity of digital public services. Because e-government platforms support essential government functions, prolonged service interruptions may reduce operational efficiency, delay service delivery, and undermine public confidence in digital government initiatives. Similarly, incidents involving unauthorized access and data loss present risks to the confidentiality and integrity of government information, which remain fundamental objectives of information security (NIST, 2018).

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

These findings are consistent with recent evidence on cybersecurity risks affecting public-sector organizations. Hossain et al. (2024) identified unauthorized access, service disruption, ransomware, and malware among the most persistent cybersecurity threats confronting local governments, emphasizing that many institutions continue to experience operational vulnerabilities despite adopting basic technical safeguards. Likewise, Prümmer et al. (2024) noted that organizations with limited cybersecurity awareness and incident preparedness are more likely to experience delayed detection and ineffective responses to cybersecurity events, thereby increasing operational and financial risks.

The qualitative findings reinforce these observations. Interview participants reported delayed incident reporting, inconsistent security monitoring, and limited coordination of incident response across departments. These findings indicate that the county's incident management capability remains insufficiently mature. Effective incident response requires not only appropriate technical tools but also clearly defined procedures, effective communication channels, and coordinated organizational responsibilities to ensure timely containment and recovery.

From a socio-technical perspective, these findings demonstrate that cybersecurity incidents arise through the interaction of technological vulnerabilities, organizational processes, and human behavior rather than from technological weaknesses alone. The findings are also consistent with the NIST Cybersecurity Framework, which emphasizes the Detect, Respond, and Recover functions as essential components of organizational cyber resilience (NIST, 2018). Similarly, ISO/IEC 27035-1:2023 highlights structured incident management, coordinated response processes, and continual improvement as critical to minimizing the operational impact of cybersecurity incidents.

Overall, the findings suggest that improving cybersecurity preparedness requires county governments to complement preventive security controls with comprehensive incident management practices encompassing continuous monitoring, timely detection, coordinated response, and effective recovery. Strengthening these capabilities would enhance the resilience of county e-government systems and support the reliable delivery of digital public services.

Organizational Factors Associated with Cybersecurity Preparedness

The Pearson correlation analysis revealed statistically significant positive associations between cybersecurity preparedness and four organizational factors: cybersecurity awareness, confidence in county cybersecurity systems, policy adherence, and the frequency of cybersecurity awareness programs. Among these variables, policy adherence demonstrated the strongest relationship with cybersecurity preparedness, followed by the frequency of cybersecurity awareness programs and confidence in county cybersecurity systems. Although cybersecurity awareness exhibited the weakest correlation, the relationship remained statistically significant, suggesting that each of these organizational factors contributes to strengthening cybersecurity preparedness.

The strong association between policy adherence and cybersecurity preparedness highlights the central role of organizational governance in achieving effective cybersecurity outcomes. While technical safeguards provide essential protection for information systems, their effectiveness depends on consistent implementation, monitoring, and enforcement of organizational policies. Well-defined cybersecurity policies establish standardized procedures for access management, incident response, acceptable system use, and regulatory compliance, thereby reducing risks associated with inconsistent user behavior and operational practices. Similar observations were

reported by Hossain et al. (2024), who identified governance and policy implementation as critical determinants of cybersecurity maturity within local government institutions.

The positive relationship between the frequency of cybersecurity awareness programs and cybersecurity preparedness further emphasizes the importance of continuous employee development. Regular awareness initiatives reinforce secure workplace practices, improve employees' ability to recognize evolving cyber threats, and promote compliance with organizational security requirements. These findings are consistent with Prümmer et al. (2024), who reported that sustained cybersecurity education enhances employees' preparedness to identify and respond to cyber threats, thereby strengthening organizational security culture. Likewise, van den Berg et al. (2025) demonstrated that continuous cybersecurity training contributes to long-term improvements in employee security behavior and organizational resilience.

Confidence in county cybersecurity systems also showed a strong positive relationship with cybersecurity preparedness. This finding suggests that employees' perceptions of system security are associated with broader organizational cybersecurity practices and governance structures. However, confidence alone should not be interpreted as evidence of actual cybersecurity capability. The descriptive findings revealed that respondents expressed relatively high confidence in county cybersecurity systems despite reporting deficiencies in staff training, incident reporting, and routine risk assessments. This disparity highlights the importance of complementing perception-based indicators with objective assessments of governance practices, technical controls, and operational performance to obtain a comprehensive understanding of organizational cybersecurity preparedness.

Although cybersecurity awareness demonstrated the weakest correlation among the variables examined, its statistically significant relationship with preparedness underscores the importance of employee knowledge in supporting organizational cybersecurity. Awareness alone is unlikely to produce meaningful improvements unless reinforced by effective governance structures, continuous training, and institutional support. This finding supports the socio-technical systems perspective adopted in this study, which views cybersecurity preparedness as the product of interactions among people, technology, and organizational processes rather than any single component operating independently.

Collectively, these findings align with the NIST Cybersecurity Framework (NIST, 2018), which emphasizes governance, awareness, continuous improvement, and organizational risk management as interconnected elements of cybersecurity preparedness. Similarly, ISO/IEC 27001:2022 and ISO/IEC 27005:2022 recognize policy implementation, employee competence, and continuous risk management as essential components of an effective information security management system. The findings therefore suggest that strengthening cybersecurity preparedness within county governments requires balanced investment in governance structures, workforce development, policy implementation, and technical safeguards.

Implications for County E-Government Systems

The findings of this study have important implications for strengthening cybersecurity preparedness within county e-government systems in Kenya and other developing countries pursuing digital transformation. Although foundational technical controls, including access control mechanisms and routine data backup procedures, have been implemented, the findings demonstrate that technical safeguards alone are insufficient to ensure organizational cybersecurity preparedness. Sustainable cybersecurity requires an integrated approach that combines technological controls with effective governance, continuous workforce development, and institutional commitment to cybersecurity risk management.

The significant positive relationships observed between cybersecurity preparedness and policy adherence, cybersecurity awareness programs, and confidence in county cybersecurity systems emphasize the importance of organizational governance in supporting secure digital service delivery. These findings suggest that county governments should prioritize the implementation and

consistent enforcement of cybersecurity policies, institutionalize continuous staff awareness and training programs, and conduct regular cybersecurity risk assessments as part of routine organizational operations. Such initiatives would strengthen organizational resilience while improving the continuity, availability, and reliability of public digital services.

The findings also have important implications for policymakers responsible for implementing Kenya's Digital Government Strategy and the national cybersecurity agenda. As county governments continue to expand digital service delivery, cybersecurity preparedness should be incorporated into institutional planning, budgeting, performance monitoring, and governance frameworks rather than being viewed solely as an information technology function. Integrating cybersecurity into organizational decision-making is likely to enhance resilience, reduce operational disruptions, and strengthen public confidence in digital government services.

From a theoretical perspective, this study reinforces the socio-technical systems perspective by demonstrating that cybersecurity preparedness is influenced by the interaction of technological, organizational, and human factors. The findings support the growing body of cybersecurity governance research, which increasingly recognizes cybersecurity as an organizational capability requiring coordinated governance, workforce competence, and continuous improvement rather than solely technological investment (NIST, 2018; Hossain et al., 2024).

The study also contributes to the growing body of knowledge on cybersecurity preparedness within public-sector organizations in developing countries. Whereas previous studies have often focused on individual technical controls or specific cybersecurity threats, this study provides empirical evidence demonstrating the combined influence of organizational governance, employee awareness, policy implementation, and institutional practices on cybersecurity preparedness within a devolved government context. Consequently, the findings contribute to addressing a gap in the literature on county-level e-government systems, which remain comparatively underrepresented in cybersecurity preparedness research.

Overall, the findings suggest that strengthening cybersecurity preparedness within county governments requires a coordinated governance approach that integrates technical safeguards, organizational policies, workforce capacity development, and continuous risk management. Such an approach is essential for enhancing the resilience, reliability, and long-term sustainability of e-government systems while supporting the secure delivery of digital public services.

Conclusion

This study assessed cybersecurity preparedness within Bomet County's e-government systems by examining three interrelated dimensions: technical security controls, organizational governance, and human capacity. The findings indicate that the county demonstrates a moderate level of cybersecurity preparedness. Although foundational security measures, particularly access control mechanisms and routine data backup practices, have been implemented, significant gaps remain in staff training, cybersecurity awareness, policy implementation, incident management, and the institutionalization of regular cybersecurity risk assessments. These deficiencies limit the county's ability to anticipate, detect, respond to, and recover from increasingly sophisticated cyber threats.

The findings further demonstrate that effective cybersecurity preparedness extends beyond the implementation of technical safeguards. Organizational factors, particularly policy adherence, cybersecurity awareness programs, and confidence in county cybersecurity systems, exhibited significant positive relationships with cybersecurity preparedness. These results reinforce the socio-technical systems perspective by demonstrating that sustainable cybersecurity depends on the interaction of technological controls, organizational governance, and human capabilities rather than on technology alone.

This study contributes to the growing body of knowledge on cybersecurity preparedness within Kenya's devolved governments, an area that remains comparatively underexplored. By providing empirical evidence from Bomet County, the study offers practical insights that can support evidence-based decision-making, strengthen cybersecurity governance, and enhance workforce

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

capacity within county governments. The findings also provide a useful foundation for improving the resilience, security, and sustainability of digital public service delivery in similar public-sector contexts.

Recommendations

The following recommendations are derived from the empirical findings of this study and are intended to strengthen cybersecurity preparedness within county e-government systems.

Strengthen Cybersecurity Governance

County governments should strengthen cybersecurity governance by enhancing the implementation and enforcement of cybersecurity policies, establishing clear governance structures, and defining responsibilities for cybersecurity oversight. Regular compliance audits and management reviews should be conducted to ensure consistent policy implementation and accountability across all departments. Cybersecurity should also be integrated into institutional planning and organizational risk management processes.

Enhance Cybersecurity Awareness and Workforce Capacity

County governments should institutionalize continuous cybersecurity education for both technical and non-technical staff. Regular awareness programs, practical training sessions, and cybersecurity simulation exercises should be conducted to improve employees' ability to recognize and respond to evolving threats, including phishing, ransomware, and social engineering attacks. These initiatives should promote a culture of shared responsibility for protecting organizational information assets.

Institutionalize Continuous Cybersecurity Risk Assessment

Structured and periodic cybersecurity risk assessments should be incorporated into routine ICT governance processes. Regular assessments will enable county governments to identify vulnerabilities, evaluate emerging threats, prioritize mitigation strategies, and continuously improve their cybersecurity posture through proactive risk management.

Strengthen Cybersecurity Monitoring and Incident Response

County governments should enhance their incident management capabilities by establishing formal incident reporting procedures, implementing continuous security monitoring, and developing comprehensive incident response plans. Clearly defined reporting mechanisms, assigned responsibilities, and regular simulation exercises would improve organizational readiness and strengthen coordinated responses to cybersecurity incidents.

Strengthen Technical Security Controls

Technical security controls should be continuously improved through timely patch management, secure system configuration, multi-factor authentication, regular vulnerability assessments, and continuous monitoring of critical information systems. These initiatives should be aligned with internationally recognized frameworks, including the NIST Cybersecurity Framework, ISO/IEC 27001:2022, and ISO/IEC 27005:2022, to support standardized cybersecurity governance and continual improvement.

Suggestions for Future Research

This study focused on cybersecurity preparedness within a single county government and examined one aspect of a broader Design Science Research project. Consequently, the findings should be interpreted within the context of Bomet County and may not be fully generalizable to all county governments in Kenya or other public-sector institutions.

Future studies should extend this research by examining cybersecurity preparedness across multiple county governments to facilitate comparative analyses and improve the generalizability of the findings. Comparative studies involving counties with different levels of digital maturity would provide deeper insights into the organizational and contextual factors influencing cybersecurity preparedness.

Further research should also investigate the effectiveness of cybersecurity governance frameworks, evaluate the long-term impact of cybersecurity awareness and workforce capacity-building initiatives on organizational resilience, and assess the implementation of

Received 21/06/2026; Revised 14/07/2026; Accepted 30/09/2026

cybersecurity risk assessment models in supporting secure and sustainable e-government service delivery. In addition, longitudinal studies would provide valuable evidence on how cybersecurity preparedness evolves over time and how sustained organizational interventions influence resilience in county e-government systems.

Declaration of Funding Sources

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Authorship Contribution Statement

Felody Chepkirui: Conceptualization, Methodology, Data Collection, Data Analysis, Writing – Original Draft.
James Abila: Supervision, Methodology, Writing – Review & Editing.
Lameck Ronoh: Supervision, Methodology, Writing – Review & Editing.

Declaration of Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Acknowledgements

The authors wish to acknowledge the County Government of Bomet for granting access to data and facilitating the data collection process. Appreciation is also extended to all respondents who participated in this study for their valuable time and insights.

References

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Communications Authority of Kenya. (2023). *Cybersecurity report 2023*. https://www.ca.go.ke

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu

Gupta, A., Sharma, R., & Singh, P. (2021). Cyber risk management models: A review and framework. *Journal of Cybersecurity Technology, 5*(2), 85–102.

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local government cybersecurity landscape: A systematic review and conceptual framework. *Applied Sciences, 14*(13), Article 5501. https://doi.org/10.3390/app14135501

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. ISO. https://www.iso.org/standard/80585.html

International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023 Information security, cybersecurity and privacy protection—Information security incident management—Part 1: Principles of incident management*. ISO.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Mushtaq, S., & Shah, M. (2024). Critical factors and practices in mitigating cybercrimes within e-government services: A rapid review on optimising public service management. *Information, 15*(10), Article 619. https://doi.org/10.3390/info15100619

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Norris, D. F., Mateczun, L., Hatcher, W., Meares, W. L., & Heslen, J. (2024). Local government cyber insecurity: Causes and recommendations for improvement. *Public Administration Review,*

84(4), 651–665. https://doi.org/10.1111/puar.13743

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, Article 103585. https://doi.org/10.1016/j.cose.2023.103585

Republic of Kenya. (2019). *Data Protection Act* (No. 24 of 2019). Government Printer.

Republic of Kenya. (2022). *National Cybersecurity Strategy 2022–2027*. Government of Kenya.

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. https://doi.org/10.1007/s11165-016-9602-2

van den Berg, M., Sommestad, T., Karlzén, H., & Pousette, A. (2025). Training for improved information security culture: A longitudinal randomized controlled trial. *Information & Computer Security, 33*(5), 690–718. https://doi.org/10.1108/ICS-08-2024-0189