INTERNATIONAL JOURNAL OF INNOVATION, ENTERPRISE, AND SOCIAL SCIENCES

ISSN 2454-6186
Volume 5, Issue 1, Pages 446-464, November, 2025
Journal Website: https://scholarnestpublishers.com/index.php/IJIESS

CYBER SECURITY RISKS AND PERFORMANCE OF COMMERCIAL STATE CORPORATIONS IN KENYA

[1] Ali Abdirahman Ibrahim, [2] Dr. Noor Ismail-PhD

[1] Msc. Scholar In Information Communication Technology Management of Jomo Kenyatta University of Agriculture and Technology, Kenya

[2] Lecturer, Jomo Kenyatta University of Agriculture and Technology, Kenya

ABSTRACT

Cybersecurity threats have become a critical challenge for commercial state corporations (CSCs) in Kenya as these organizations expand their digital infrastructure to enhance service delivery, operational efficiency, and public accountability. Despite national frameworks such as the Kenya National Cybersecurity Strategy (2022–2027) and the Data Protection Act (2019), recent audits reveal that the majority of CSCs lack formal cybersecurity policies, testing procedures, and dedicated security budgets, exposing them to risks that compromise service continuity and regulatory compliance. The main objective of this study was to examine the influence of cybersecurity risks on the performance of commercial state corporations in Kenya. Specifically, the study sought to assess the effect of network security and regular testing and updates on organizational performance indicators such as service availability, stakeholder satisfaction, and legal compliance. The study was grounded in the Technology–Organization–Environment (TOE) Framework and Dynamic Capabilities Theory. A quantitative, cross-sectional survey research design was employed, targeting all 46 CSCs in Kenya. A purposive sampling approach was used to select a sample of 92 respondents, comprising ICT managers and strategic planning officers. Data was collected using semi-structured questionnaires and analysed using SPSS version 27. A pilot study involving 10 respondents from five non-participating commercial state corporations were conducted to assess the clarity, consistency, and construct alignment of the structured questionnaire, with expert reviews ensuring content validity and reliability confirmed through Cronbach's alpha using SPSS. For the main study, descriptive statistics including frequencies, percentages, means, and standard deviations summarized the data, while inferential statistics such as Pearson's correlation and multiple linear regression were used to examine relationships between variables. Network security emerged as the most influential factor, followed by regular testing and updates. The study concluded that effective cybersecurity management enhances operational efficiency, service reliability, regulatory compliance, and stakeholder trust. It emphasized that cybersecurity is not merely a technical function but a strategic performance enabler for public-commercial institutions. The study recommends that commercial state corporations invest in robust network protection systems and implement structured testing and update policies. Strengthening these practices holistically will enhance resilience, ensure service continuity, and improve the overall performance of commercial state corporations in Kenya.

Key Words: Cybersecurity Risks, Commercial State Corporations in Kenya, Network Security, Regular Testing and Updates, Organizational Performance

Background of the Study

The increasing reliance on digital technologies by public sector institutions has elevated cybersecurity from a peripheral IT concern to a core element of strategic governance and national resilience. In Kenya, commercial state corporations, entities owned by the government but operating on commercial principles, play a vital role in supporting national infrastructure, delivering essential services, and facilitating socio-economic development (Kazee & Mahomed, 2024). As these organizations expand their digital footprints to enhance operational efficiency and stakeholder engagement, they have also become more exposed to cyber risks that threaten data integrity, service continuity, and institutional credibility (Kshetri, 2024).

The Communications Authority of Kenya (CAK) reported over 700 million cyber threat events in 2023 alone, a figure that highlights both the scale and aggressiveness of malicious actors targeting Kenya's digital infrastructure. These threats range from phishing, malware, ransomware, and insider threats to large-scale Distributed Denial of Service (DDoS) attacks that paralyze service delivery in critical state institutions (CAK, 2023). Furthermore, the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC) confirmed that public-sector institutions remain among the top targeted sectors in the country, with repeated vulnerabilities observed due to inconsistent cyber hygiene practices and inadequate response protocols (KE-CIRT/CC, 2023).

Despite these alarming trends, cybersecurity remains under-prioritized in many Kenyan state corporations. A 2022 audit by the ICT Authority and the Office of the Auditor General revealed that 67% of commercial state corporations lacked formal cybersecurity policies, 82% had never conducted penetration testing, and only 18% had dedicated cybersecurity budgets (Serianu, 2023). Additionally, 90% of the surveyed organizations lacked operational cybersecurity incident response plans, leaving them highly vulnerable to both technical disruptions and reputational harm.

These institutional weaknesses persist despite existing national policy frameworks such as the Kenya National Cybersecurity Strategy (2022–2027) and the enforcement of legal statutes like the Data Protection Act (2019), which mandates public entities to protect personal data and respond appropriately to breaches (ODPC Kenya, 2022). The disconnect between digital service expansion and cybersecurity preparedness underscores a critical governance and operational risk for Kenya's public sector.

The situation in Kenya mirrors global trends. The IBM X-Force Threat Intelligence Index (2023) noted a 94% increase in cyberattacks targeting government sectors globally, with African nations among the most vulnerable due to inadequate cyber maturity models. In Kenya's case, while financial institutions have made significant strides in securing digital infrastructure, spurred by regulatory oversight, public sector organizations, especially commercial state corporations, remain under-studied and under-protected (Kimuyu & James, 2024). This imbalance is further evidenced in literature. Most African cybersecurity research tends to focus on banking, fintech, or private telecommunications, with limited empirical data on public-commercial entities (Ndegwa & Moyo, 2022). Yet, commercial state corporations are uniquely vulnerable. They carry dual accountability: commercial competitiveness on one hand and public service obligations on the other. This duality makes them attractive targets for cybercriminals while demanding higher standards of governance.

The gap is also functional. According to Bikundo and Mwangi (2021), most public agencies in Kenya still rely on reactive cybersecurity measures, rarely conducting penetration tests, vulnerability scans, or staff capacity building. Similarly, Ombati and Njoroge (2022) found that compliance-based approaches often supersede performance-based cybersecurity integration, leaving systems poorly adapted to emerging threats. This study, therefore, sought to empirically investigate the extent to which cybersecurity practices, network security, continuous threat

monitoring, and regular testing and updates, affect the performance of commercial state corporations in Kenya. By grounding the investigation in real-world challenges and aligning with international standards and practices, the research aims to provide evidence-based insights that can inform national cybersecurity governance, policy development, and operational strategies.

Statement of the Problem

In the face of rapid digital transformation, Kenya's commercial state corporations have increasingly adopted technology to enhance service delivery, streamline operations, and expand stakeholder engagement. However, this shift has introduced new vulnerabilities, with cyber threats now posing significant risks to the stability, efficiency, and credibility of these institutions. The nature and volume of cybersecurity incidents targeting public sector entities in Kenya have escalated at an alarming rate. The Communications Authority of Kenya (CAK) reported that the country experienced over 860 million cyber threat events in Q3 of 2023, a 34.5% increase from the previous quarter. Among these were 278 million malware detections, 109 million botnet activities, and 4,537 DDoS attacks, many directed at public institutions and infrastructure (CAK, 2023).

Despite government efforts such as the National Cybersecurity Strategy (2022–2027) and the implementation of legal frameworks like the Data Protection Act (2019), cybersecurity preparedness across commercial state corporations remains inadequate. An audit conducted in 2022 by the ICT Authority and the Office of the Auditor-General revealed that 67% of state corporations lacked a formal cybersecurity policy, 82% had never conducted penetration testing, and only 18% had dedicated cybersecurity budgets. Furthermore, 90% of public institutions lacked an operational cybersecurity incident response plan (CSIRP) (Serianu, 2023). These lapses expose corporations to service outages, data breaches, reputational damage, and financial loss, all of which negatively impact performance metrics such as service uptime, customer satisfaction, compliance, and cost-efficiency.

Several empirical studies have emphasized the impact of cybersecurity practices on organizational performance, particularly in developing economies. For example, Aldrighetti et al. (2021) found that real-time network monitoring significantly reduced operational disruptions in public utilities in South Africa. Ombati & Njoroge (2022), in their study on Kenyan government agencies, identified that poor implementation of regular testing and updates was a major contributor to system vulnerabilities and data loss. Munyua et al. (2023) also revealed that cybersecurity governance had a statistically significant effect on the performance of semi-autonomous government agencies, especially in terms of public trust and service continuity.

However, most existing studies on cybersecurity within the public sector tend to concentrate on broader themes such as IT governance, regulatory frameworks, or specific sectors like healthcare and financial services, while giving limited attention to the distinctive operational structure of commercial state corporations entities expected to be both commercially viable and publicly accountable. For instance, Ombati and Njoroge (2022) focused on cybersecurity compliance in regulatory agencies, while Munyua et al. (2023) investigated cybersecurity governance within health-focused parastatals. Additionally, Ndegwa and Moyo (2022) examined policy gaps across East African public agencies but did not address performance-related metrics or organizational competitiveness. None of these studies examined the combined effect of cybersecurity practices such as network security and regular testing and updates on the performance outcomes of commercial state corporations. This represents a critical research gap. This study sought to fill this critical gap by providing data-driven insights into how cybersecurity risks influence performance of commercial state corporations in Kenya.

Objectives of the Study

General Objective

To examine the influence of cybersecurity risks on the performance of commercial state corporations in Kenya.

Specific Objectives

i. To examine the influence of network security on the performance of commercial state corporations in Kenya.

ii. To evaluate the effect of regular testing and updates on the performance of commercial state corporations in Kenya.

LITERATURE REVIEW

Theoretical Review

Technology–Organization–Environment (TOE) Framework

The Technology–Organization–Environment (TOE) Framework, developed by Tornatzky and Fleischer (1990), provides a comprehensive model for understanding how organizations adopt and implement technological innovations. According to the framework, three distinct but interrelated contexts shape organizational decisions regarding technology adoption: the technological context, the organizational context, and the environmental context. Each of these dimensions plays a vital role in determining whether, how, and to what extent a particular technology, such as a cybersecurity solution, is adopted and effectively utilized.

In the technological context, TOE examines the internal and external technologies available to the organization, emphasizing features such as complexity, compatibility, and relative advantage (Oliveira & Martins, 2011). For cybersecurity, this relates to the nature of network security tools such as firewalls, intrusion prevention systems (IPS), encryption protocols, and access control mechanisms. The organizational context focuses on internal characteristics such as top management support, ICT infrastructure, technical expertise, and firm size, all of which affect readiness for secure system adoption (Zhu & Kraemer, 2005). Finally, the environmental context refers to external pressures, including regulatory requirements, industry competition, risk exposure, and customer expectations all highly relevant in shaping cybersecurity priorities (Yoon, 2021).

The TOE framework is widely regarded in ICT and information systems research due to its flexibility and applicability across sectors and technological types (Baker, 2012). In the field of cybersecurity, TOE has been used to explain variations in the adoption of network security measures among public institutions, SMEs, and healthcare systems. For instance, Alshamaila, Papagiannidis, and Li (2013) applied the framework to explain cloud security adoption in public agencies, showing that organizational readiness and environmental uncertainty were more significant than technical features alone. Similarly, Kamau and Wairimu (2022) found that Kenyan state entities with strong leadership commitment and external pressure were more likely to adopt advanced network defense tools. Critically, the TOE framework avoids the narrow technical determinism that often plagues ICT adoption models. It acknowledges that network security is not merely a matter of purchasing the right tools, but requires strategic alignment with organizational priorities and responsiveness to external threats and regulatory standards. This perspective is particularly valuable for Kenya's commercial state corporations, which face the dual burden of public service accountability and market competitiveness. In such contexts, network security implementation depends not only on available technologies but also on institutional capabilities, cyber policy enforcement, and sector-specific threats.

However, TOE has been critiqued for its broadness and lack of prescriptive specificity (Baker, 2012). It identifies important domains of influence but does not always offer clear mechanisms for operationalizing or prioritizing factors across the three contexts. Furthermore, it may underrepresent cultural and political influences that significantly affect public-sector cybersecurity in emerging economies (Kshetri, 2021). Nonetheless, TOE remains a robust analytical lens due to its multi-dimensional structure, and its ability to integrate both technical and institutional considerations in explaining cybersecurity behavior.

In this study, the TOE framework provides a theoretically sound basis for examining how network security practices are adopted and institutionalized within Kenya's commercial state corporations. It facilitates an understanding of how the effectiveness of these cybersecurity practices depends on the interplay between system complexity, organizational readiness, and regulatory environment making it far more rigorous than purely technical frameworks such as the Defense-in-Depth principle, which lacks theoretical grounding.

Dynamic Capabilities Theory

The Dynamic Capabilities Theory (DCT), developed by Teece, Pisano, and Shuen (1997), emphasizes an organization's ability to build, integrate, and reconfigure internal competencies to respond to rapid external changes. The theory emerged as a response to the limitations of the resource-based view (RBV), which emphasized firm-level resources but did not explain how organizations adapt to turbulence and technological disruption. DCT introduced the idea that in dynamic environments, static resources are insufficient; instead, organizations must continuously sense changes, seize opportunities, and transform internal operations (Teece, 2007).

In the context of cybersecurity, regular testing and system updates are critical manifestations of dynamic capabilities. These practices enable organizations to identify vulnerabilities, assess risk exposure, and reconfigure their security architecture in response to emerging threats. Testing methods such as penetration testing, patch management, vulnerability scans, and incident simulations reflect the core DCT processes of learning and adaptation (Pillai et al., 2021). Rather than assuming a static defense model, dynamic cybersecurity emphasizes ongoing evolution of tools, policies, and practices closely aligning with the adaptive essence of DCT.

For Kenya's commercial state corporations, which operate in a complex and evolving threat landscape, dynamic capabilities are essential for maintaining resilience and institutional credibility. These organizations handle sensitive data, critical infrastructure, and public-facing services making them attractive cyber targets. Yet, as observed by Kamunde and Otieno (2022), many state corporations either lack formal testing schedules or rely on outdated tools, leaving them exposed to persistent vulnerabilities. Organizations that institutionalize routine security audits, continuous system updates, and feedback loops from previous incidents demonstrate stronger performance in maintaining service availability and minimizing cyber-related disruptions.

Empirical evidence reinforces the utility of DCT in cybersecurity management. Obwaka and Mwololo (2023) found that Kenyan public corporations with embedded testing protocols and system reconfiguration processes were more effective at recovering from ransomware attacks and minimizing system downtime. Similarly, Tallon et al. (2019) showed that dynamic capabilities positively influence digital risk management outcomes, particularly when regular review and improvement cycles are embedded into cybersecurity strategy. These findings support the proposition that regular testing and updates are not merely operational tasks, but strategic routines that sustain institutional agility in the face of cyber threats.

Nonetheless, DCT has been critiqued for conceptual ambiguity and measurement challenges. Scholars like Barreto (2010) and Winter (2003) argue that while the theory offers valuable

insights, it lacks clear operational metrics and tends to describe what organizations should do without specifying how they should do it. In resource-constrained environments like the Kenyan public sector, the absence of practical implementation guidelines may hinder the realization of dynamic capabilities, even when the theoretical rationale is sound. Moreover, the success of such routines often depends on leadership commitment, cross-functional integration, and organizational culture, all of which may vary widely among state corporations.

Despite these limitations, DCT remains highly relevant to the current study. It offers a robust framework for examining how regular testing and updates contribute to organizational performance by enabling adaptation, resilience, and continuous learning. It supports the idea that cybersecurity is not a one-time investment, but a continuous cycle of assessment, adjustment, and renewal particularly critical in high-risk, high-responsibility institutions such as Kenya's commercial state corporations.

Conceptual Framework

A conceptual framework is a structured representation of the variables, constructs, and theories guiding a study. According to Ravitch and Riggan (2016), a conceptual framework "acts as a lens through which to view the research problem, guiding the researcher in defining variables, formulating hypotheses, and interpreting findings." In this study, the framework maps out the relationship between cybersecurity risk management practices (independent variables) and organizational performance (dependent variable), while anchoring each variable in a relevant and academically validated theory.

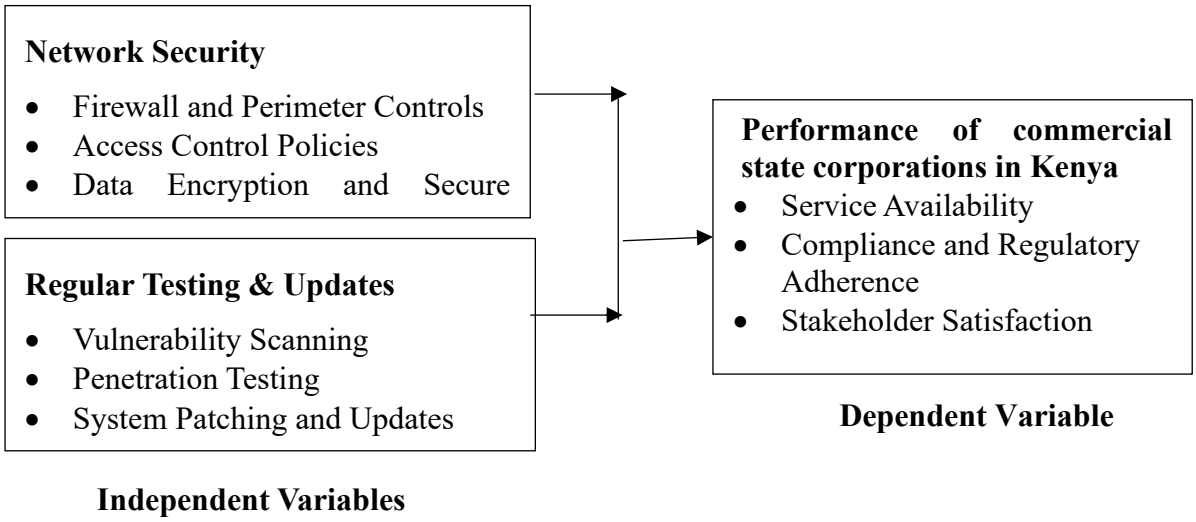

Figure 2. 1: Conceptual Framework

Network Security

Network security refers to the strategic configuration of technologies, policies, and practices designed to protect the integrity, confidentiality, and availability of organizational information as it traverses internal and external networks. In the context of commercial state corporations (CSCs), network security is central to maintaining operational continuity and institutional trust, especially given their dual obligation to both commercial efficiency and public accountability. According to Omar and Altohami (2023), robust network security mechanisms not only prevent unauthorized access but also enhance organizational performance by reducing the frequency and impact of cyber incidents.

The current study conceptualizes network security using three key indicators: firewall and perimeter controls, access control policies, and data encryption and secure transmission. Firewall and perimeter controls represent the first layer of defense against external threats. Firewalls filter network traffic based on predefined security rules and act as a gatekeeper

between trusted internal networks and untrusted external ones. These tools, including next-generation firewalls (NGFWs), are essential for defending CSCs from distributed denial-of-service (DDoS) attacks, intrusion attempts, and malware propagation. Research by Arefin et al. (2021) demonstrates that organizations with well-configured firewall systems experience significantly fewer disruptions and enhanced responsiveness to emerging threats. Moreover, Kulkarni and Akhilesh (2021) emphasize that public institutions, especially in the energy and finance sectors, must incorporate perimeter-based tools like deep packet inspection and threat intelligence filtering to safeguard mission-critical infrastructure.

Access control policies dictate who can access what information, under what circumstances, and through what levels of authentication. These policies ensure that users are only granted permissions necessary for their job functions, following the principle of least privilege (POLP). Access control mechanisms can be role-based, attribute-based, or biometric, and are critical in mitigating insider threats and limiting the damage from breached accounts. Sharma, Lashkari, and Parizadeh (2024) argue that improper access configuration remains one of the most common vulnerabilities in public sector cybersecurity breaches. They advocate for layered access models integrated with identity and access management (IAM) systems to bolster accountability and user traceability across digital operations.

Data encryption and secure transmission refer to the practice of converting information into unreadable formats during storage or transfer, only to be decrypted by authorized parties. This protects data from interception, manipulation, or leakage during network communication. Encryption protocols such as TLS, VPN tunneling, and end-to-end encryption are widely recognized as pillars of secure digital governance. In a study on cybersecurity practices in Saudi public institutions, Alhumud, Omar, and Altohami (2023) observed that data encryption significantly enhanced compliance with national digital protection regulations and increased public confidence in service delivery. Similarly, Mohsini, Toke, and Rashidi (2025) noted that African public institutions that adopted secure transmission protocols saw improvements in both data integrity and system uptime.

Overall, these network security components (firewalls, access control, and encryption) form a synergistic triad that supports proactive threat mitigation and fosters resilience in state-operated digital ecosystems. As network architectures in CSCs grow more complex due to digitization and remote service delivery, securing these systems is no longer optional but a prerequisite for sustained performance and legal compliance.

Regular Testing and Updates

Regular testing and updates form a proactive cybersecurity strategy essential for managing emerging threats and maintaining digital resilience. For commercial state corporations (CSCs) that manage large-scale digital infrastructure while maintaining public accountability, regular vulnerability assessments, testing, and system updates ensure system integrity, regulatory compliance, and operational efficiency (Admass, Munaye, & Diro, 2024). These practices help prevent attacks that exploit known weaknesses and are core to a risk-based defense posture.

Vulnerability scanning is the automated process of identifying known weaknesses in an organization's digital environment, such as unpatched software, insecure configurations, and exposed network ports. According to Süren et al. (2023), vulnerability scanning plays a pivotal role in identifying security gaps before attackers can exploit them. These scans utilize databases like the CVE (Common Vulnerabilities and Exposures) list to evaluate compliance and prioritize remediation based on risk. In public organizations, routine scans support a continuous assessment cycle, helping maintain baseline security and meet the requirements of data protection regulations (Park & Kim, 2025).

Penetration testing, also known as ethical hacking, simulates actual cyberattacks to test the resilience of systems under real-world conditions. While vulnerability scanning is often

automated and based on known issues, penetration testing involves human-led or AI-assisted exploration of unknown vulnerabilities, logic flaws, and business process weaknesses (Omar, Altohami, & Alhumud, 2023). According to Mayukha and Vadivel (2022), public-sector organizations benefit significantly from annual or quarterly penetration testing as it uncovers systemic gaps in authentication, authorization, and intrusion prevention mechanisms. It also validates whether incident response plans are actionable and effective under stress.

System patching and updates refer to the routine process of applying vendor-issued software and firmware updates to close discovered vulnerabilities. Failure to update systems in a timely manner leaves them susceptible to known exploits often the most common cause of security breaches in public institutions (Troncoso-Pastoriza et al., 2020). Liu, Huang, and Lucas (2020) found that centralized IT governance, including structured patch management policies, significantly reduces breach incidents in public institutions such as universities. Updating operating systems, applications, and embedded firmware is crucial for maintaining compatibility with emerging cybersecurity tools and for meeting government audit standards.

Moreover, Ribeiro et al. (2025) emphasize that the effectiveness of regular testing and patching increases when aligned with global frameworks such as NIST SP 800-53 or ISO/IEC 27001. Public organizations with systematic vulnerability scanning, testing, and updating procedures report higher service uptime, reduced incident costs, and greater public confidence in their digital services (Iakovakis et al., 2021). These benefits extend beyond technical performance to influence broader organizational metrics such as user satisfaction, compliance ratings, and audit readiness.

Thus, vulnerability scanning identifies what is wrong, penetration testing tests how it can be exploited, and patching ensures it is fixed together forming a robust cycle of threat management. This triad is not optional but a critical requirement for digital resilience in CSCs operating in an increasingly complex and hostile cyber landscape.

Performance of Commercial State Corporations in Kenya

Performance in the context of commercial state corporations (CSCs) is a multidimensional concept that captures the effectiveness, efficiency, and accountability of public institutions that operate under commercial mandates. In this study, performance is operationalized using three indicators: service availability, compliance with regulatory frameworks, and stakeholder satisfaction. These dimensions are particularly relevant for CSCs in Kenya, which are tasked with delivering public goods while maintaining financial viability.

Service availability refers to the capacity of CSCs to deliver uninterrupted, accessible, and reliable services to their intended users. Downtime caused by technical failures, cyberattacks, or resource constraints directly undermines this metric. As Njihia and Imende-Obonyo (2024) note, digital service continuity is essential in measuring CSC effectiveness, especially in sectors like transportation, utilities, and communications. Enhanced ICT integration without corresponding cybersecurity safeguards increases vulnerability, impacting service uptime. Automated systems for performance tracking and real-time reporting play a crucial role in maintaining service reliability and identifying operational bottlenecks (Tukamushaba, Bindeeba, & Bakashaba, 2025).

Compliance and regulatory adherence reflects the extent to which CSCs conform to government directives, legal standards, and institutional frameworks such as the Public Procurement and Asset Disposal Act (2015) and Kenya's Data Protection Act (2019). Regulatory compliance is not only a legal necessity but also a signal of good governance. According to Latiff et al. (2025), cybersecurity compliance including data protection, logging, and access control enhances institutional accountability and limits exposure to reputational and financial penalties. In Kenya, state corporations are increasingly subject to audits and oversight,

where cybersecurity alignment with ISO/IEC 27001 or NIST frameworks is an emerging performance benchmark (Ismail & Pastory, 2024).

Stakeholder satisfaction encompasses the perceptions of service users, employees, regulators, and partners concerning CSC performance. Satisfaction is influenced by factors such as system availability, transparency, responsiveness to incidents, and the quality of digital interactions. Studies show that citizens and businesses are less likely to trust and engage with state-run platforms if they experience recurrent disruptions or privacy breaches (Oroni & Xianping, 2023). Chihwai (2024) emphasizes that digital maturity and cybersecurity assurance directly shape public confidence and stakeholder engagement in government-linked enterprises.

These three dimensions represent both technical and strategic aspects of organizational performance. Ensuring continuous service, meeting legal and ethical obligations, and satisfying stakeholders are not independent activities, they intersect heavily with cybersecurity capability. As CSCs become more digitized, cyber risks increasingly influence key performance indicators. Thus, any comprehensive performance evaluation must integrate ICT governance and cybersecurity readiness as core constructs.

Empirical Literature Review

Network Security and Organizational Performance

In Vietnam, Huy and Phuc (2024) evaluated how cybersecurity investments, especially in network security infrastructure, influence performance in public-sector service delivery. The study applied a mixed-method design combining 212 structured survey responses with 12 expert interviews. The researchers found that network security measures like firewalls and intrusion prevention systems directly enhanced service reliability and citizen trust in digital government platforms. The most influential factor was robust access control frameworks, which reduced unauthorized data manipulation. However, challenges such as procurement delays and limited cross-agency collaboration were noted as hindrances to fully integrated security systems. The authors called for central ICT agencies to offer shared network security services to smaller agencies lacking technical capacity.

Regionally, Mahama, Elbashir, and Sutton (2022) explored the digital governance landscape in African state organizations, focusing on the role of ICT in performance. Using a multi-country survey approach in Ghana, Nigeria, and Uganda, they found that agencies with encrypted data flows and multi-factor authentication protocols outperformed peers in areas of regulatory compliance and digital trust. The research revealed that simple encryption-based transmission models were often more effective than complex but poorly maintained systems. Additionally, government institutions that practiced monthly access reviews were significantly more likely to meet digital service-level agreements. Despite these advances, many African governments were still reliant on outdated legacy systems vulnerable to known exploits.

Locally, in Kenya, Oroni and Xianping (2023) studied commercial state corporations to evaluate how network security influences organizational performance. Their study used structural equation modeling (SEM) on data from 142 respondents across energy, transport, and water-related CSCs. They found that firewall protection and secure access protocols strongly influenced both service uptime and compliance with the Data Protection Act (2019). Encryption practices also correlated positively with stakeholder satisfaction, especially in organizations offering digital interfaces for public use. Nonetheless, a significant challenge noted was the irregular updating of network configurations, which left systems exposed despite having otherwise good architecture. The study recommended institutionalizing periodic firewall audits and segmenting network layers based on sensitivity.

Regular Testing and Updates and Organizational Performance

In a European-wide study, Szczepaniuk, Rokicki, and Szczepaniuk (2020) assessed cybersecurity maturity in 160 public administration entities across Poland. Using quantitative scoring models aligned with ISO/IEC 27001 standards, the research emphasized that regular testing (such as monthly vulnerability scans) was significantly associated with successful Information Security Management System (ISMS) implementation. Institutions that performed quarterly patch updates and conducted annual penetration tests showed a 40% improvement in audit compliance and disaster recovery readiness. Nonetheless, the researchers observed that without a centralized repository for patch and test logs, information silos remained a risk, reducing interdepartmental accountability.

Regionally, in Ghana, Yusif and Hafeez-Baig (2021) examined cybersecurity governance in state-controlled universities and public utilities. They developed a conceptual model linking organizational cybersecurity culture to operational performance. Regular testing routines particularly penetration tests and security backups were found to reduce recovery time during incidents and increase end-user trust. The study reported that performance gains were maximized in institutions that coupled system patching with employee training. Still, a lack of national testing mandates and limited vendor oversight in public procurement posed challenges to standardization across institutions.

Locally, in Kenya, Oroni and Xianping (2023) conducted an empirical evaluation of cybersecurity practices across eight commercial state corporations, focusing specifically on regular testing and update protocols. Their Structural Equation Modeling (SEM) analysis revealed that organizations conducting quarterly vulnerability scans and system patching were 36% more likely to achieve full compliance with the Data Protection Act (2019). These organizations also reported improved financial performance due to fewer system downtimes and reduced incidence of ransomware attacks. The study recommended formalizing update policies and creating internal audit units specifically tasked with evaluating the frequency and effectiveness of testing activities.

RESEARCH METHODOLOGY

This study adopted a descriptive cross-sectional research design to examine the relationship between cybersecurity risks and the performance of commercial state corporations in Kenya. This design is appropriate for analyzing variables at a single point in time and enables broad generalization across the target population of state corporations (Creswell & Creswell, 2018). The unit of analysis was the commercial state corporation, while the units of observation was the ICT Manager and the Strategic Planning Officer from each organization. The ICT Manager provides technical insights into cybersecurity practices, while the Strategic Planning Officer offers a performance-oriented view. Selecting these two roles ensures a balanced assessment of both cybersecurity implementation and its effect on organizational outcomes. This approach yields a total of 92 respondents (2 per corporation), providing sufficient coverage for valid statistical analysis while ensuring relevance and depth of responses.

This study adopted a census sampling approach by including all 46 commercial state corporations located in Nairobi City County, as recognized by the State Corporations Advisory Committee (SCAC, 2019). A census is ideal in this context due to the relatively small population size, and because it allows for complete sector-wide coverage, thereby enhancing both the external validity and generalizability of the findings (Mugenda & Mugenda, 2003).

This study utilized a semi-structured questionnaire as the main instrument for primary data collection. A pilot study was conducted with approximately 10% of the total sample, involving 10 respondents drawn from 5 commercial state corporations that were not participate in the main survey. This preliminary step is essential for testing the clarity, consistency, and usability

of the questionnaire before full-scale deployment (Kumar, 2019). It assessed whether the items are clearly worded, logically structured, and appropriately aligned with the constructs of cybersecurity risk management and organizational performance.

Data analysis was conducted using SPSS Version 27, combining both descriptive and inferential statistics (Kothari, 2019). Descriptive analysis (means, standard deviations, frequencies) summarized responses on each cybersecurity practice and performance indicator. To examine the relationship between cybersecurity risk management practices and organizational performance, Pearson's correlation assessed association strength, and multiple linear regression determined predictive influence. Significance was tested at the 95% confidence level ($p < 0.05$), and ANOVA assessed the overall model fit. Results were presented through tables, bar charts, and narrative interpretation.

RESEARCH FINDING AND DISCUSSION

Out of the 92 questionnaires distributed to ICT managers and strategic planning officers across the 46 commercial state corporations, 85 were duly completed and returned, representing a response rate of 92.4%. This high response rate was achieved through consistent follow-ups and electronic submissions, reflecting strong engagement and reliability of the collected data. According to Mugenda and Mugenda (2003), a response rate above 70% is considered excellent for academic research; therefore, the obtained rate was adequate for statistical analysis

Descriptive Analysis

Network Security

This subsection presents the descriptive analysis of the second independent variable, network security, which evaluates the extent to which commercial state corporations implement technical and policy measures to safeguard their network infrastructure, control access, and ensure secure data transmission. Respondents rated eight statements relating to network security practices, and the results are summarized in Table 1.

Table 1: Descriptive Statistics for Network Security

Statement	Mean	Std. Deviation
Our organization uses firewalls to protect internal systems.	4.200	0.814
Access to systems is controlled through role-based permissions.	4.118	0.877
Data transmitted across networks is encrypted.	4.059	0.904
Network security is reviewed and updated regularly.	3.965	0.926
There is a formal policy governing access control.	4.071	0.889
Devices connecting to the network are subject to authentication checks.	3.988	0.915
Intrusion detection systems are in place.	3.929	0.931
Security patches are installed across all network components.	3.976	0.904
Aggregate Score	**4.038**	**0.895**

Source: Research Data (2025)

The findings indicate that network security practices are generally well established among commercial state corporations in Kenya. The highest-rated statement was the use of firewalls to protect internal systems (Mean = 4.200, SD = 0.814), demonstrating strong perimeter defense mechanisms. Similarly, access to systems through role-based permissions (Mean = 4.118, SD = 0.877) and encryption of transmitted data (Mean = 4.059, SD = 0.904) scored

highly, suggesting that most organizations have implemented structured access controls and secure communication protocols.

Moderately high means were recorded for the existence of access control policies (Mean = 4.071, SD = 0.889) and authentication of devices connecting to the network (Mean = 3.988, SD = 0.915). This indicates a growing culture of accountability and authentication in system access management. However, slightly lower scores were observed in areas related to intrusion detection systems (Mean = 3.929, SD = 0.931) and regular security reviews (Mean = 3.965, SD = 0.926), implying that while the foundational tools are in place, continuous auditing and automated intrusion response may still be underdeveloped in some corporations.

The overall aggregate mean of 4.038 (SD = 0.895) signifies that respondents agreed to a high extent that network security practices are implemented across commercial state corporations. This suggests that most entities have adopted proactive security infrastructures and policies to safeguard their networks against cyber threats.

These findings agree with the conclusions of Said et al. (2023), who observed that organizations with robust firewalls, secure data transmission protocols, and regular network audits achieved stronger operational resilience and faster recovery from cyber incidents. Similarly, Mahama, Elbashir, and Sutton (2022) found that institutions employing encryption and multi-factor authentication recorded better digital trust and compliance outcomes. The consistency between these findings and the current study underscores the critical role of layered network defenses and continuous policy enforcement in improving organizational performance and safeguarding public-sector digital assets.

Regular Testing and Updates

This subsection presents the descriptive analysis of the fourth independent variable, regular testing and updates, which examines how frequently commercial state corporations conduct vulnerability scans, penetration testing, and system updates to maintain cybersecurity resilience. Respondents rated eight statements reflecting their organizations' practices related to cybersecurity testing and system updates. The results are presented in Table 2.

Table 2: Descriptive Statistics for Regular Testing and Updates

Statement	Mean	Std. Deviation
Regular vulnerability scans are conducted across IT systems.	4.012	0.876
Penetration testing is performed periodically.	3.941	0.895
Systems and applications are patched promptly when updates are available.	4.118	0.861
Software updates follow a documented change management process.	3.976	0.910
System components are tested for resilience after every major update.	3.965	0.923
Update cycles are scheduled and adhered to consistently.	3.988	0.905
Backups are verified as part of the testing and update process.	4.047	0.883
Cybersecurity testing outcomes inform decision-making and improvement.	4.024	0.867
Aggregate Score	**4.009**	**0.890**

Source: Research Data (2025)

The results show that commercial state corporations in Kenya conduct regular testing and updates to a high extent. The highest mean score was recorded for timely patching of systems and applications (Mean = 4.118, SD = 0.861), indicating strong adherence to software update

cycles as a preventive cybersecurity measure. Similarly, the verification of backups (Mean = 4.047, SD = 0.883) and the use of testing outcomes for decision-making (Mean = 4.024, SD = 0.867) scored highly, reflecting a structured approach to maintaining data integrity and continuous improvement.

Moderate to high means were observed for conducting vulnerability scans (Mean = 4.012, SD = 0.876) and adherence to update schedules (Mean = 3.988, SD = 0.905), suggesting that although most corporations perform regular scans, resource and technical constraints might affect consistency across all systems. Penetration testing (Mean = 3.941, SD = 0.895) and post-update system resilience testing (Mean = 3.965, SD = 0.923) were slightly lower, implying that while these practices exist, they may not yet be institutionalized as routine components in every organization's cybersecurity program.

The overall aggregate mean of 4.009 (SD = 0.890) indicates that respondents generally agreed to a high extent that regular testing and updates are performed. This implies that Kenya's commercial state corporations have embraced continuous system improvement and proactive maintenance, enhancing their ability to mitigate vulnerabilities before they are exploited. These findings agree with those of Liu, Huang, and Lucas (2020), who established that structured patch management and centralized IT governance significantly reduce cybersecurity incidents in public institutions. Likewise, Ribeiro et al. (2025) observed that organizations aligning their testing and updating practices with international standards such as ISO/IEC 27001 report higher service availability and stakeholder confidence. The consistency between these studies and the present findings suggests that routine system testing and timely updates are critical drivers of operational continuity and digital trust within public-commercial institutions.

Organizational Performance

This subsection presents the descriptive analysis of the dependent variable, organizational performance, which assessed how cybersecurity practices influence service availability, compliance, and stakeholder satisfaction in commercial state corporations. Respondents were asked to indicate their level of agreement with eight statements measuring various aspects of performance linked to cybersecurity management. The results are presented in Table 3.

Table 3: Descriptive Statistics for Organizational Performance

Statement	Mean	Std. Deviation
Our organization maintains high service availability through digital platforms.	4.118	0.871
Cybersecurity has improved operational continuity.	4.071	0.883
The organization complies with national ICT and data protection regulations.	4.047	0.902
Users and stakeholders are satisfied with our information systems.	4.000	0.918
There is minimal downtime due to cybersecurity-related incidents.	3.929	0.945
Cybersecurity practices support strategic planning and execution.	4.059	0.879
The organization demonstrates resilience during cybersecurity crises.	4.035	0.891
Cybersecurity contributes to our reputation and stakeholder trust.	4.129	0.862
Aggregate Score	4.049	0.894

Source: Research Data (2025)

The results show that respondents generally agreed to a high extent that effective cybersecurity practices have positively influenced the performance of commercial state corporations. The highest-rated statement was that cybersecurity contributes to organizational reputation and stakeholder trust (Mean = 4.129, SD = 0.862), underscoring the reputational and confidence-

building role of strong cybersecurity frameworks. Similarly, high service availability (Mean = 4.118, SD = 0.871) and improved operational continuity (Mean = 4.071, SD = 0.883) indicate that cybersecurity measures have enhanced system uptime and reliability across digital platforms.

Compliance with national ICT and data protection laws (Mean = 4.047, SD = 0.902) and strategic integration of cybersecurity into planning processes (Mean = 4.059, SD = 0.879) further reveal that security governance has become an embedded component of institutional management. On the other hand, slightly lower mean scores were observed for minimal downtime due to cybersecurity incidents (Mean = 3.929, SD = 0.945) and stakeholder satisfaction (Mean = 4.000, SD = 0.918), suggesting that while overall performance is strong, occasional disruptions and user concerns may still occur due to evolving cyber threats or system upgrades.

The aggregate mean of 4.049 (SD = 0.894) reflects agreement to a high extent, indicating that commercial state corporations in Kenya are achieving strong performance outcomes through structured and proactive cybersecurity practices. These results demonstrate that cybersecurity has evolved from a technical safeguard to a strategic performance driver, directly enhancing efficiency, compliance, and institutional credibility. These findings agree with those of Shaheen and Waqar (2024), who observed that mature cybersecurity postures in public organizations strengthen operational continuity and public confidence by safeguarding data and minimizing downtime. Similarly, Njihia and Imende-Obonyo (2024) found that enhanced ICT governance and security maturity significantly improve service reliability and accountability in public enterprises. The present study therefore reinforces the notion that robust cybersecurity management directly supports organizational performance, ensuring that commercial state corporations remain resilient, compliant, and trusted in Kenya's digital governance ecosystem.

Correlation Analysis

This subsection presents the results of the Pearson correlation analysis, which was conducted to determine the strength and direction of the relationships between each cybersecurity practice, network security and regular testing and updates, and the performance of commercial state corporations in Kenya. Correlation coefficients (r) range between –1 and +1, where values close to +1 indicate a strong positive relationship, those near 0 indicate no relationship, and those near –1 show a strong negative relationship. The following interpretation scale was used: 0.00 – 0.19: Very Weak Relationship, 0.20 – 0.39: Weak Relationship, 0.40 – 0.59: Moderate Relationship, 0.60 – 0.79: Strong Relationship, 0.80 – 1.00: Very Strong Relationship. A significance level (p-value) of less than 0.05 was used to determine statistical significance. The results are summarized in Table 4.

Table 4: Correlation Analysis Results

		Performance	Network Security	Regular Testing and Updates
Performance of Commercial State Corporations	Pearson Correlation	1		
	Sig. (2-tailed)			
	N	85		
Network Security	Pearson Correlation	.781**	1	
	Sig. (2-tailed)	.000		
	N	85	85	
Regular Testing and Updates	Pearson Correlation	.772**	.461**	1
	Sig. (2-tailed)	.000	.000	
	N	85	85	85

The correlation analysis revealed a strong positive and statistically significant relationship between network security and performance (r = 0.781, p = 0.000). This suggests that organizations that implement robust network defenses, such as firewalls, access controls, and encryption protocols, achieve superior performance due to reduced system breaches and higher data protection standards. Enhanced network security safeguards digital assets, minimizes downtime, and fosters stakeholder trust. These results agree with Szczepaniuk et al. (2020), who found that well-secured networks strengthen reliability and institutional performance through better risk containment. Likewise, Huy and Phuc (2024) emphasized that secure network configurations promote efficiency and digital trust in public agencies, reinforcing the evidence that network security is integral to the performance of commercial state corporations in Kenya.

The analysis revealed a strong positive and statistically significant relationship between regular testing and updates and performance (r = 0.772, p = 0.000). This means that consistent vulnerability testing, patch management, and system updates significantly enhance efficiency and reliability in commercial state corporations. Regular testing ensures that weaknesses are identified early, while prompt updates keep systems resilient against emerging threats. These results are supported by Mayukha and Vadivel (2022), who found that structured penetration testing and patching schedules enhance public organizations' operational continuity and user confidence. Likewise, Troncoso-Pastoriza et al. (2020) observed that timely system updates reduce vulnerability exposure and maintain service stability, reinforcing the strong linkage found in this study.

Regression Analysis

Table 5: Regression Coefficients

Predictor	Unstandardized Coefficient (B)	Std. Error	Standardized Coefficient (β)	t-value	p-value
(Constant)	0.215	0.092	,	2.337	0.022
Network Security	0.298	0.078	0.273	3.821	0.001
Regular Testing and Updates	0.256	0.076	0.237	3.361	0.003

Dependent Variable: Performance of Commercial State Corporations in Kenya
Source: Research Data (2025)

Network Security (B = 0.298, β = 0.273, p = 0.001). Network security has the largest standardized beta (0.273), showing it is the most influential predictor of performance. A one-unit increase in network security practices, such as strengthening firewalls, encryption, and access controls, leads to a 0.298-unit improvement in performance. This implies that a secure and resilient network environment is central to the sustainability and operational excellence of commercial state corporations. The significance of this variable aligns with Kshetri (2024), who found that robust network architectures significantly enhance institutional reliability and public confidence in digital systems.

Regular Testing and Updates (B = 0.256, β = 0.237, p = 0.003). The results indicate that a one-unit increase in regular testing and updates improves the performance of commercial state corporations by 0.256 units. The standardized beta (0.237) also confirms its strong predictive role. This means that organizations conducting frequent vulnerability scans, penetration testing, and timely system updates enhance resilience and service availability. These findings agree with Asare and Boateng (2023), who established that consistent system updates and structured testing significantly enhance operational continuity and data integrity in public enterprises.

Based on the unstandardized coefficients presented in Table 4.15, the estimated multiple regression equation for the study is expressed as follows:

$$Y = 0.215 + 0.298X_1 + 0.256X_2 + \varepsilon$$

Where: Y= Performance of Commercial State Corporations in Kenya, X_1= Network Security, X_2= Regular Testing and Updates, 0.215= Constant (intercept), and ε= Error term

Conclusions

Second, network security emerged as the most influential factor affecting performance. Corporations that implement robust network protection measures, including encryption, firewalls, and access control, experience fewer breaches and higher operational stability. This underscores the central role of secure digital infrastructure in maintaining data integrity and stakeholder trust.

Lastly, regular testing and updates were found to enhance performance by ensuring systems remain resilient against evolving threats. Periodic vulnerability scans, penetration tests, and timely software updates strengthen cybersecurity readiness, reduce risk exposure, and promote uninterrupted organizational operations.

Recommendations

Network Security

The study recommends that commercial state corporations enhance their network security by investing in modern technologies and adopting layered defense strategies. This includes the use of next-generation firewalls, encryption protocols, and multi-factor authentication to safeguard access and data transmission. Institutions should also ensure that access control policies are periodically reviewed and updated to match changes in organizational roles and system architecture. Furthermore, routine network security audits should be conducted to identify and seal vulnerabilities before they are exploited. To reinforce these efforts, partnerships with reputable cybersecurity firms can be established for expert assessment and capacity development.

Regular Testing and Updates

The study recommends that commercial state corporations adopt structured policies for regular system testing and updates to maintain robust cybersecurity postures. Vulnerability scanning, penetration testing, and patch management should be conducted consistently, with clear documentation and follow-up on identified weaknesses. Organizations should implement automated patch deployment tools to ensure timely updates and minimize human error. Moreover, the outcomes of security tests should be analyzed and used to inform improvement in system design and operational policies. Management should also enforce strict compliance with change management procedures to prevent unauthorized modifications that could compromise system stability.

Areas for Further Research

This study focused on the influence of cybersecurity practices on the performance of commercial state corporations in Kenya. Future research could extend this work by examining the role of organizational culture, leadership commitment, and employee behavior in shaping cybersecurity effectiveness. Comparative studies across different sectors or East African countries could also provide broader insights into regional cybersecurity maturity. Additionally, future studies could explore the moderating effects of emerging technologies such as artificial intelligence, blockchain, or cloud computing on the relationship between cybersecurity management and institutional performance, offering a deeper understanding of how digital innovation interacts with security frameworks to drive organizational success.

REFERENCES

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications, 4*(1), 1–18.

Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach. *Cogent Education, 10*(1), 2265227.

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the UK: A multivariate analysis of TOE framework. *Journal of Enterprise Information Management, 26*(3), 250–275.

Arefin, M. T., Uddin, M. R., Evan, N. A., & Alam, M. R. (2021). Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). In *Intelligent networks, big data and IoT* (pp. 749–764). Springer.

Asare, P., & Boateng, M. (2023). Cybersecurity risk management practices and performance of public institutions in Ghana. *African Journal of Information Systems, 15*(1), 1–19.

Baker, J. (2012). The technology–organization–environment framework. In Y. Dwivedi et al. (Eds.), *Information systems theory* (pp. 231–245). Springer.

Barreto, I. (2010). Dynamic capabilities: A review of past research and an agenda for the future. *Journal of Management, 36*(1), 256–280.

Bikundo, O., & Mwangi, F. (2021). Cybersecurity preparedness in Kenyan public sector institutions: Gaps and governance issues. *Journal of Public Sector ICT Governance, 5*(1), 41–58.

Chihwai, P. (2024). Digital innovation adoption in South African national parks, hotels, and airports. In *Tourism and hospitality for sustainable development* (pp. 37–52). Springer.

Communications Authority of Kenya. (2023). *Q3 cybersecurity report 2023*. https://ca.go.ke

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

ICT Authority, & Office of the Auditor General. (2022). *ICT audit report on cybersecurity preparedness in state corporations*. Government of Kenya.

Iakovakis, G., Xarhoulacos, C. G., Giovas, K., & Papamichail, M. (2021). Analysis and classification of mitigation tools against cyberattacks in the COVID-19 era. *Security and Privacy, 4*(3), e3187205.

Ismail, A. M., & Pastory, D. (2024). Evaluating the impact of self-service cash deposit machines on the performance of commercial banks in Tanzania. *Future Business Journal, 10*(1), 21–37.

Kamau, S., & Wairimu, H. (2022). Determinants of cybersecurity adoption in Kenya's public sector: A TOE perspective. *African Journal of Information Systems, 14*(2), 1–19.

Kamunde, P., & Otieno, L. (2022). Cybersecurity adaptability and organizational resilience in Kenya's public sector. *East African Journal of ICT Governance, 4*(1), 41–58.

Kazee, N., & Mahomed, A. (2024). NHLS cyber-attack: Untold costs. Have we learned? *Wits Journal of Clinical Medicine, 6*(3), Article 7.

Kimuyu, S., & James, R. (2024). Cybersecurity investment patterns in Kenya: A sectoral analysis. *East African Journal of Policy Research, 5*(1), 19–38.

Kothari, C. R. (2019). *Research methodology: Methods and techniques* (4th ed.). New Age International.

Kultar, S. (2019). *Research methodology and statistical techniques*. Deep & Deep Publications.

(You cited "Kumar, 2019" in the text, but what you actually listed is Kultar, 2019. Right now your in-text and reference don't match.)

Latiff, A. R., Alqudah, M. Z., Samara, H., & Alslaibi, N. (2025). Empowering the financial sector: The role of fintech research development trends. *Future Business Journal, 11*(1), Article 512.

Liu, C. W., Huang, P., & Lucas, H. C., Jr. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems, 37*(3), 714–740.

Mahama, H., Elbashir, M., & Sutton, S. (2022). Enabling enterprise risk management maturity in public sector organizations. *Public Money & Management, 42*(4), 266–277.

Mayukha, S., & Vadivel, R. (2022). Reconnaissance for penetration testing using active scanning of MITRE ATT&CK. In *ICTCS 2021: Intelligent computing and communication* (pp. 685–699).

Mohsini, M., Toke, F. V., & Rashidi, F. (2025). Framework for enhancing effectiveness of information security measures implemented in public institutions in Tanzania. *The Electronic Journal of Information Systems in Developing Countries, 91*(3), e70017.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. Acts Press.

Munyua, J., Kimani, D., & Karanja, L. (2023). Cybersecurity governance and service delivery in Kenyan health parastatals. *Journal of Public Sector ICT Management, 5*(2), 91–107.

Ndegwa, M., & Moyo, T. (2022). Public sector cybersecurity capacity in East Africa: Policy gaps and institutional readiness. *African Governance and Development Review, 6*(1), 55–72.

Njihia, J. M., & Imende-Obonyo, V. (2024). User readiness as a determinant for use of big data analytics: A case of state corporations in Kenya. *The Electronic Journal of Information Systems in Developing Countries, 90*(3), e12327.

Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach. *Cogent Education, 10*(1), 2265227.

(You duplicated this one in the long list; once is enough.)

Obwaka, M., & Mwololo, J. (2023). Dynamic cyber capabilities and service continuity in Kenyan state corporations. *Journal of African Public Sector Innovation, 6*(1), 19–35.

Ombati, A., & Njoroge, S. (2022). Evaluating cybersecurity compliance in Kenyan public regulatory bodies. *East African Journal of Information Security, 4*(1), 23–38.

Oroni, C. Z., & Xianping, F. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance. *Journal of Data, Information and Management, 5*(4), 245–261.

Park, J., & Kim, T. S. (2025). A framework to improve the compliance guideline for critical ICT infrastructure security. *Journal of Open Innovation: Technology, Market, and Complexity, 11*(1), 82.

Pillai, S., Meshram, P., & Khan, M. (2021). Cybersecurity capabilities and threat intelligence: A dynamic capability perspective. *Information & Computer Security, 29*(5), 907–926.

Ribeiro, M. … (2025).

You gave only “Ribeiro et al. (2025)” with no full bibliographic details. To make this APA-compliant you must supply full author list, article title, journal, volume, issue, and pages. Right now it’s incomplete.

Said, R. A., Taleb, N., Al Blooshi, I. A., & Alamim, A. S. (2023). IT governance and control: Mitigation and disaster preparedness of organizations in the UAE. In *The effect of information technology on organizational performance* (pp. 607–619). Springer.

State Corporations Advisory Committee. (2019). *Directory of state corporations in Kenya*. Government of Kenya.

Serianu. (2023). *Africa cybersecurity report: Kenya edition*. https://serianu.com

Shaheen, A., & Waqar, S. (2024). Higher education and cyber-crime perception among university students in Islamabad. *Apex Journal of Social Sciences, 3*(2), 44–52.

Shaikh, F. A., & Siponen, M. (2024). Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions. *Information Systems Frontiers, 26*(1), 89–106.

Sharma, D. P., Lashkari, A. H., & Parizadeh, M. (2024). Understanding cybersecurity management in healthcare. In *Progress in information systems* (pp. 145–168). Springer.

Szczepaniuk, E. K., Szczepaniuk, H., & Rokicki, T. (2020). Information security assessment in public administration. *Computers & Security, 93*, 101790.

Tallon, P. P., Queiroz, M., Coltman, T., & Sharma, R. (2019). Information technology and the search for organizational agility: A systematic review. *The Journal of Strategic Information Systems, 28*(2), 218–237.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350.

Teece, D. J. (2014). The foundations of enterprise performance: Dynamic and ordinary capabilities in an (economic) theory of firms. *Academy of Management Perspectives, 28*(4), 328–352.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Troncoso-Pastoriza, J. R., Argaw, S. T., Lacey, D., Flor, A. F., & Ralston, W. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1), 146.

Tukamushaba, E. K., Bindeeba, D. S., & Bakashaba, R. (2025). Digital transformation and its multidimensional impact on sustainable business performance: Evidence from a meta-analytic review. *Future Business Journal, 11*(1), Article 511.

World Bank. (2022). *Cybersecurity and public sector resilience in Africa*. Author.

Yoon, C. (2021). Determinants of cybersecurity capability development in public institutions: A TOE-based approach. *Government Information Quarterly, 38*(4), 101596.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance: Application in Ghana's public universities. *Journal of Applied Security Research, 16*(3), 329–346.

Zhu, K., & Kraemer, K. L. (2005). Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry. *Information Systems Research, 16*(1), 61–84.