2025

Perceived effects of cybersecurity culture on financial performance of Kenyan commercial banks: moderated by audit committee characteristics.

Ngei, Eric Mutunga
Strathmore Business School
Strathmore University

PERCEIVED EFFECTS OF CYBERSECURITY CULTURE ON FINANCIAL PERFORMANCE OF KENYAN COMMERCIAL BANKS: MODERATED BY AUDIT COMMITTEE CHARACTERISTICS

ERIC MUTUNGA NGEI

MBA/168419

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE AWARD OF DEGREE OF MASTER OF BUSINESS ADMINISTRATION OF STRATHMORE UNIVERSITY

MAY 2025

DECLARATION

I declare that this dissertation is my original work and has not been previously submitted and approved by Strathmore University or any other Institution for the award of a degree. To the best of my knowledge and belief, this dissertation is original and borrowed materials have been done with due reference.

ERIC MUTUNGA NGEI

Approval

This dissertation of Eric Mutunga Ngei was approved by the following:

Name of Supervisor: Dr. James Ndegwa

School/Institute/Faculty: Strathmore University Business School

Dr. Ceaser Mwangi

Executive Dean

Strathmore University Business School

Prof. Bernard Shibwabo

Director, Office of Graduate Studies

Strathmore University

ABSTRACT

Commercial banks in Kenya, like many institutions globally, face a growing number of cyber threats that could severely impact their financial stability, customer trust, and operational effectiveness. Over the years, the financial performance of Tier II and Tier III commercial banks in Kenya has been on the decline. This study sought to establish the effect of cybersecurity culture on the performance of commercial banks in Kenya, moderated by audit committee characteristics. The objectives of the study were to determine the effect of top management support on performance of commercial banks in Kenya, to examine the effect of information security policy on performance of commercial banks in Kenya, to investigate the effect of cyber security training on performance of commercial banks in Kenya and to assess the moderating effect of audit committee characteristics on the relationship between cybersecurity culture and performance of commercial banks in Kenya. The study was anchored on the institutional theory, the resource-based view and the agency theory. The study adopts a positivist philosophy. A descriptive research design was used, involving a cross-sectional survey. The research targeted 38 commercial banks in Kenya. A random sampling technique was employed, to select a sample size of 114 employees. A structured questionnaire was used to gather data on a 5-point Likert scale. Financial performance data was obtained from reports from the Central Bank of Kenya. Descriptive statistics (mean, standard deviation) was used, followed by multiple regression analysis to assess the influence of cybersecurity culture factors on the banks' performance. The study revealed that top management support, information security policies within the commercial banks and cybersecurity training have a significant positive effect on the financial performance of commercial banks in Kenya. The audit committee characteristics significantly moderates the relationship between cybersecurity initiatives and financial performance. The Central Bank of Kenya should develop and enforce cybersecurity governance guidelines that mandate minimum standards for management involvement and audit oversight in cybersecurity. There is need to implement policies that require the continuous review and updating of information security policies at least annually. Commercial banks management should aim to improve the relevance and applicability of cybersecurity training.

Key words: financial performance, cybersecurity, culture, management, training, audit, policy

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

C3SA	Cybersecurity Capacity Centre for Southern Africa
CAMEL	Capital adequacy, Asset quality, Management quality, Earnings, and Liquidity
CBK	Central Bank of Kenya
CCO	Chief Cybersecurity Officer
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CLV	Customer Lifetime Value
CMA	Capital Markets Authority
CR	Cyber Regulations
CSD	Cybersecurity Disclosure
CSI	Customer Satisfaction Index
EBIT	Earnings Before Interest and Taxes
ESG	Environmental, Social, and Governance
EU	European Union
GDPR	General Data Protection Regulation
IDV	Individualism
IVR	Indulgence
KE-CIRT	Kenya's National Kenya Computer Incident Response Team
KM	Knowledge Management
LTO	Long-Term vs. Short-Term
MAS	Masculinity
NPLs	Non-Performing Loans
NPS	Net Promoter Score
NSE	Nairobi Securities Exchange
PDI	Power Distance

RBV	Resource-Based View
ROA	Return on Assets
ROE	Return on Equity
SEC	Securities and Exchange Commission
SMEs	Small to Medium-sized Enterprises
SP	Security Policies
UAI	Uncertainty Avoidance

DEFINITION OF TERMS

Audit Committee characteristics	The structural, operational, and behavioral attributes of an audit committee within an organization that influence its effectiveness in overseeing financial reporting, internal controls, risk management, and other critical areas, including cybersecurity (Usman et al., 2024).
Cyber Security Culture	The set of values, beliefs, and practices related to protecting an organization's information assets from cyber threats (D'Arcy & Hovav, 2009). The beliefs, values, knowledge, assumptions, perceptions, norms and attitudes of people towards cybersecurity and how they manifest in their interaction with information technologies (European Union Agency for Network and Information Security (ENISA), 2017).
Cybersecurity Training	The process of educating employees, users, or other stakeholders about cybersecurity principles, threats, best practices, and how to protect sensitive data and systems (Fagbule, 2023).
Financial performance	Refers to how well a company or organization is performing in terms of its financial outcomes. It is typically measured using various key financial indicators and metrics that provide insight into its profitability, revenue generation, cost management, and overall financial health (Kaplan & Norton, 1992).
Information Security Policy	A formalized set of guidelines, rules, and procedures established by an organization to ensure the confidentiality, integrity, and availability of its information assets (Alraja et al., 2023).
Top Management Support	The active involvement, endorsement, and commitment of an organization's senior leadership in driving and sustaining a particular initiative or strategy (Obogi & Kiarie, 2019).

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The global banking industry has undergone profound changes over the past few decades, primarily driven by advances in technology, regulatory shifts, and evolving customer needs (Murinde et al., 2022). Traditionally, the banking sector was characterized by physical branches and paper-based transactions. However, the emergence of digital banking, fintech innovations, and the rapid adoption of mobile technologies have reshaped the landscape of financial services worldwide. Banks now operate in a more interconnected, digital-first environment, offering online banking, mobile payments, peer-to-peer lending, and blockchain-based solutions (Gomber et al., 2022).

Despite the enormous benefits brought by digital transformation, the global banking sector faces significant challenges, primarily cyber threats. As the world becomes increasingly digitized, cyber-attacks targeting financial institutions have escalated. Cybersecurity has become a critical concern for governments, businesses, and individuals worldwide (Georgiadou et al., 2022). High-profile data breaches, ransomware attacks, and fraud incidents have become a frequent occurrence, undermining customer trust and threatening the stability of financial institutions.

In response, banks globally have had to adopt stronger cybersecurity measures to protect sensitive financial data, comply with regulations, and mitigate risks. The role of cybersecurity culture, which is an organization's collective efforts to safeguard information through awareness, behaviour, and actions, has become an essential component of the broader security framework (Aksoy, 2024). Institutions now recognize that technology alone cannot secure banking systems without fostering a proactive cybersecurity culture among employees, customers, and leadership.

The financial sector in Kenya, particularly commercial banks, has undergone significant transformation over the past decade, driven by technological advancements, regulatory changes, and evolving consumer behaviour. However, alongside these developments, the rise in cybercrime and the increasing complexity of cyber threats have posed substantial risks to the financial industry, including banks. In an era where banking is increasingly digital, cybersecurity has become an essential pillar for the growth and survival of financial institutions. In the recent report, 840,921,998 cyber threats were detected by the National KE-

CIRT/CC between October and December 2024 (The National KE-CIRT/CC, 2025). This was a 27.82% rise compared to the previous quarter (July-Sep, 2024). During the period, systems attacks were at over 750 million incidents, brute force were over 34 million, malware was over 33 million cases, DDOS attacks were over 15 million, and web app attacks were over 4 million. According to the report, the majority of these threats occur in the financial sector (The National KE-CIRT/CC, 2025).

In today's digital economy, cybersecurity has become a critical determinant of financial performance, particularly within the banking sector, where institutions handle vast amounts of sensitive financial data (Erondu & Erondu, 2023). The rise in cyber threats such as phishing, ransomware, and data breaches poses significant operational and reputational risks to banks, which can lead to substantial financial losses, regulatory penalties, and erosion of customer trust. As such, a strong cybersecurity culture plays a pivotal role in safeguarding digital assets and maintaining operational continuity. When effectively implemented, cybersecurity measures not only reduce the incidence and cost of cyberattacks but also enhance efficiency, customer confidence, and overall financial outcomes (Teoh & Mahmood, 2017).

Cybersecurity incidents in the banking sector globally and within Kenya have highlighted the critical vulnerabilities in the systems and processes that are designed to protect sensitive financial data. These breaches have often resulted in considerable financial losses, reputational damage, and a loss of customer trust (Agina, 2022). In Kenya, commercial banks have been targets of cyber-attacks, including data breaches, financial fraud, and system infiltrations. For instance, high-profile cases such as the hacking of mobile banking applications and ATM fraud have put a spotlight on the banks' ability to safeguard their systems and assets.

As more Kenyans turn to mobile banking services, commercial banks are increasingly using digital metrics, such as mobile money transactions and online banking usage rates, to measure customer satisfaction and loyalty. A 2021 report by the Central Bank of Kenya (CBK) showed that mobile banking usage in Kenya has grown by over 45% annually, highlighting the importance of digital services for banks' performance (CBK, 2021).

The financial performance of Kenyan commercial banks has exhibited notable inconsistencies over the years, influenced by a wide range of internal and external factors. For instance, the total assets in the banking sector stood at Ksh. 7.7 trillion in 2023 surging by Ksh. 1.2 trillion while asset quality deteriorated in 2023, with non-performing loans (NPLs) rising to 14.8% of gross loans, the highest since 2007 (KBA, 2024). In December 2023, profit before tax stood at

Ksh. 219.2 billion which was 8.8% decrease compared to Ksh. 240.4 billion in December 2022. This drop in profitability signals a challenging year for the banking sector overall. Total income increased by Ksh. 154.1 billion, while total expenses increased by Ksh. 175.3 billion. The increase in expenses outpaced income growth. This imbalance between income and expenses suggests that banks are facing higher operational costs without being able to generate proportional revenue to offset these expenses (CBK, 2023).

While some banks have shown impressive growth and profitability, others have struggled with issues such as rising Non-Performing Loans (NPLs), low capital reserves, and increasing competition from fintech companies. Larger banks like Equity Bank and KCB have been successful in leveraging technology, expanding mobile banking services, and enhancing their digital platforms. On the other hand, smaller and less agile banks have faced challenges in maintaining competitiveness and customer loyalty, leading to uneven performance across the sector.

Tier 1 banks (the largest in Kenya) dominate performance from both non-financial and financial perspectives of the banking industry, accounting for approximately 80% of the sector's performance. This is a clear indication that the remaining 20% is divided among smaller, often less financially stable Tier 2 and Tier 3 banks. For Tier 2 and Tier 3 banks, there is a crisis in terms of financial performance, cybersecurity preparedness, and overall market competitiveness. A report by the KBA (2023) shows that the Tier 2 and Tier 3 banks have been performing poorly as compared to the large banks. The report highlights that large banks (Tier 1) outperformed medium (Tier 2) and small (Tier 3) banks in terms of lending growth. Lending by large banks grew by 14.7% to Kshs. 2.8 trillion, while medium banks saw a 9.1% increase to Kshs. 472 billion. In contrast, small banks experienced a decline of 2.9%, with their lending dropping to Kshs. 264.2 billion. This indicates that medium and small banks are performing poorly compared to the large banks in loan growth.

According to CBK (2023), Tier 1 banks increased their combined market share to 76.6 per cent in December 2023 from 75.1 per cent in December 2022. The combined market share of Tier 2 banks decreased to 15.0 per cent in December 2023, from 16.3 per cent in December 2022. Tier 3 banks (Small Peer group) had a combined market share of 8.4 per cent in December 2023, a decrease from 8.61 per cent in December 2022. The value of mortgage loans outstanding increased by Ksh. 19.7 billion (7.5%) from Ksh. 261.8 billion in December 2022 to Ksh. 281.5 billion in December 2023. This growth indicates a healthy expansion in the mortgage market overall. However, a significant 89.5% of the mortgage market lending was

concentrated in just 9 institutions. Of these 9 institutions, 6 were large banks, contributing 76.4% of the lending, while 2 medium-sized banks accounted for 13.1%. This shows a strong dominance of large banks in the mortgage market. In the previous year, 83% of the mortgage lending was also concentrated in 8 institutions. Out of the 8, 7 were large banks (with 75% of the lending), while only 1 medium-sized bank contributed 8%. This further shows that large banks have maintained or even slightly strengthened their dominant position in the mortgage market.

As evident, Tier 1 banks already perform well and can often absorb financial or cybersecurity risks better than smaller banks. These smaller banks may struggle more with resources, cybersecurity culture, and organizational management, which makes them more vulnerable to systemic risks. However, this is not documented and thus the need for this study to assess the effect of cyber security culture on the financial performance of commercial banks in Kenya; moderated by audit committee characteristics.

1.1.1 Cyber Security Culture

A cybersecurity culture refers to the collective mindset, values, and behaviours shared by individuals within an institution that prioritize the protection of information and technological infrastructure from cyber threats (Aksoy, 2024). According to Corradini (2020), cybersecurity culture represents the collective behaviour and attitudes towards safeguarding digital assets, information, and systems from cyber threats. Building a strong cybersecurity culture is essential in ensuring that every member of an organization is aware of and actively contributes to mitigating cybersecurity risks. A positive cybersecurity culture is seen as essential to mitigate risks such as data breaches, cyberattacks, and identity theft (Mwim & Mtsweni 2022). The foundation of a strong cybersecurity culture in banks often stems from top leadership commitment, staff training, awareness programs, and well-defined security protocols. The increasing recognition that technological systems are only as secure as the people who operate them has driven banks to prioritize building such a culture.

Alnatheer's (2014) conceptual model identified top management support, effective information security policy, information security training, information security risk analysis and assessment and ethical conduct policies as the key constructs of a cybersecurity culture. Top management support, effective information security policy and information security training were ranked as the topmost constructs that conceptualize cybersecurity culture. According to Sutton and Tompson (2024), a strong cybersecurity culture means that every individual in the organization

recognizes the importance of cybersecurity in their daily work, adheres to security policies and practices, is cognizant of potential risks and mitigations, promotes a security-conscious environment, where reporting incidents or suspicious activities is encouraged and receives regular training to stay updated on cybersecurity threats and best practices.

Hofstede (2010) identified six dimensions of culture for understanding cultural differences across countries. These dimensions explain how values in the workplace are influenced by culture. The six dimensions are Power Distance (PDI), Individualism (IDV), Masculinity (MAS), Uncertainty Avoidance (UAI), Long-Term vs. Short-Term (LTO) and Indulgence (IVR). The six dimensions reflect different ways in which national cultures can vary and how these differences impact interactions, management, and organizational behavior.

Globally, organizations have increasingly recognized the importance of creating strong cybersecurity cultures. According to the World Economic Forum (WEF) (2022) report, cyberattacks have become one of the top global risks, with over 60% of companies reporting a cyber-incident in the past year. This highlights the growing recognition of cybersecurity risks and the need for organizations to establish a strong security culture. This is supported by a study from Cisco's 2021 Cybersecurity Readiness Index which found that only 15% of global organizations had fully integrated cybersecurity culture into their operations, emphasizing a significant gap in many organizations' readiness to tackle cyber threats (Cisco, 2021).

Globally, companies are investing heavily in employee cybersecurity training programs. This trend is driven by the fact that human error continues to be one of the top causes of cybersecurity breaches. More organizations are recognizing the importance of top management's involvement in cybersecurity. It is no longer just an IT issue but a strategic organizational priority. With the rise in cybercrime, more organizations are turning to cybersecurity insurance to mitigate financial risks, though the global cybersecurity insurance market is expected to grow by 10.5% annually from 2023 to 2030. The rise in cyberattacks has highlighted the importance of a robust cybersecurity culture. According to IBM Security (2023), the average cost of a data breach has reached $4.24 million.

In Europe, the General Data Protection Regulation (GDPR) has raised awareness about the significance of data protection, prompting organizations to take cybersecurity more seriously. A report by Eurostat (2021) revealed that 71% of European companies experienced cyber incidents, with small businesses being particularly vulnerable due to limited resources and awareness. In North America, the United States is a leader in developing a robust cybersecurity

culture, largely due to its technological infrastructure and ongoing legislative initiatives. However, the Cybersecurity & Infrastructure Security Agency (CISA) has reported that critical sectors, such as healthcare and energy, remain underprepared (Bronk & Conklin, 2022). Canada, on the other hand, has adopted a more proactive approach with national cybersecurity strategies and the promotion of cyber hygiene practices (AlDaajeh et al., 2022).

In Africa, cybersecurity culture is still emerging. According to a UNCTAD (2020) report, 87% of African countries had some form of cybersecurity law in place, but enforcement and the widespread cultural adaptation to cybersecurity practices lag behind. Regional cybersecurity capacity building is still needed, especially as cyber threats like ransomware are becoming more prevalent across the continent. The Cybersecurity Capacity Centre for Southern Africa (C3SA) (2021) reports that many organizations in Southern Africa have limited awareness and weak governance frameworks, hindering the region's ability to foster a robust cybersecurity culture**.**

Locally, in Kenya, cybersecurity is increasingly recognized as a national concern. The Kenya Computer Misuse and Cybercrimes (Amendment) Bill passed in 2021, provides a framework for dealing with cybersecurity issues at the national level. However, the local cybersecurity culture remains in its nascent stages, particularly within smaller businesses and public sector institutions. According to the Kenya National ICT Survey (2021), only 40% of Kenyan companies had formal cybersecurity policies in place, and even fewer (around 25%) conducted regular security awareness training for employees. This demonstrates the ongoing struggle to build a comprehensive cybersecurity culture that permeates all levels of organizations. Kenya's National Kenya Computer Incident Response Team (KE-CIRT) (2020), reported that cybercrime cases in the country have been increasing. Similarly, according to Statista (2024), cybercrimes in Kenya increased to more than 700 million in 2022, which was 69 percent more than the prior year. This is reported especially in sectors such as banking and telecommunications. A rise in phishing scams, mobile fraud, and ransomware attacks has made it clear that more attention needs to be given to cybersecurity awareness and cultural integration.

Prior studies on cybersecurity culture have investigated several key aspects, though with notable gaps in context and scope. Top management support has been examined by Obogi and Kiarie (2019), Roustapisheh and Yazdizadeh (2022), and Mukaila et al. (2022), focusing on leadership commitment and strategic prioritization of cybersecurity; however, these studies mainly explored general organizational performance in non-banking sectors like schools,

hospitals, and software firms, without directly linking leadership support to financial performance in banks. Information security policy was addressed by Kong et al. (2023) and Alzahrani and Seth (2021), who highlighted its role in safeguarding data and promoting organizational stability, yet their work focused on SMEs and securities firms outside Africa, limiting relevance to Kenya's commercial banking sector. Cybersecurity training was explored by Kweon et al. (2021) and Fagbule (2023), emphasizing awareness and incident reduction but not clearly connecting training to financial outcomes. On the moderating effect of audit committee characteristics, studies like Matemane et al. (2024) and Alodat et al. (2024) discussed the influence of board expertise and diversity on cybersecurity governance and disclosures, but did not explicitly test their moderating role between cybersecurity culture and financial performance. However, this study intends to focus on the effect of cybersecurity culture (top management support, cyber security training, information security policy) on the financial performance of commercial banks in Kenya.

Alnatheer's (2014) conceptual model justifies the choice of variables based on the significant role each plays in shaping and sustaining a cybersecurity culture. Top management support, information security policy, and cybersecurity training are key elements that influence organizational behavior and contribute directly to a secure environment. The audit committee's moderating role adds a layer of governance that ensures these practices are properly implemented and maintained, which aligns with the model's emphasis on organizational structure and oversight in creating a strong cyber security culture.

1.1.2 Audit Committee Characteristics

The concept of Audit Committee Characteristics refers to the attributes or qualities of the audit committee within an organization that determine how effectively it oversees financial reporting, internal controls, risk management, and other key governance functions (Bepari, 2023). The key audit committee characteristics that are often studied in the context of corporate governance are expertise, independence, size of the committee, meeting frequency, diversity (including gender diversity), tenure and experience of members, responsiveness and engagement with cybersecurity issues and interaction with external auditors (Mardessi, 2021; Al-Jalahma, 2022).

Independence is one of the most frequently emphasized characteristics of an effective audit committee. An independent audit committee is free from any influence or interference from the organization's executive management. Research has shown that an independent audit

committee is more likely to make objective decisions and provide unbiased oversight, especially in areas such as risk management and financial reporting (Bananuka & Nkundabanyanga, 2023; Boshnak, 2021). The expertise of audit committee members, particularly in finance, accounting, or cybersecurity, is a critical characteristic influencing the committee's effectiveness. Experts are better positioned to evaluate financial statements, assess risks, and understand the complex issues surrounding cybersecurity. Research has shown that the presence of members with financial or technical expertise can lead to more informed decision-making and improved governance (Oussii & Boulila, 2021).

The size of the audit committee has been another characteristic discussed in the literature. Some studies argue that larger audit committees are more effective because they bring diverse perspectives and can share the workload more efficiently (Fariha, Hossain & Ghosh, 2022). Others suggest that smaller committees are more agile and can make decisions more quickly without the complexity of coordinating a large group. Research findings on this characteristic have been mixed, with some studies showing no direct link between size and committee effectiveness (Ha, 2022).

The frequency of meetings held by the audit committee is another important characteristic. A higher number of meetings is often associated with more rigorous oversight and the ability to address emerging issues in a timely manner. Studies have shown that audit committees that meet more frequently are better able to provide effective oversight, monitor risks, and respond to financial irregularities and cybersecurity threats (Gupta & Mahakud, 2021). According to Mardessi (2021), a longer tenure might indicate more experience and a deeper understanding of the institution's operations, but it could also lead to potential complacency or a lack of fresh perspectives. On the other hand, short tenure might bring more dynamic insights but less institutional knowledge. Research suggests that a balance of tenure is necessary to ensure effective oversight (Azizkhani et al., 2023).

Globally, audit committees have increasingly been scrutinized for their ability to provide effective oversight on not just financial reporting but also operational risks, cybersecurity, and Environmental, Social, and Governance (ESG) concerns. There is a growing emphasis on cybersecurity oversight, with audit committees being urged to take a more active role in monitoring and addressing cybersecurity risks. This has become a prominent issue for multinational companies, especially after high-profile data breaches and cyberattacks. The Securities and Exchange Commission (SEC) in the United States, has begun requiring greater disclosures related to cybersecurity risks and incidents. As a result, audit committees in many

U.S. firms are increasingly expected to oversee the implementation of cybersecurity frameworks (Davalos & Feroz, (2022). The European Union (EU) has implemented stringent regulations around data protection and digital privacy (Cervi, 2022). According to Hermanson et al. (2024), audit committees globally are becoming more diverse, with a focus on including members with varied expertise (e.g., cybersecurity, technology, law, finance). Gender and ethnic diversity are also receiving increasing attention.

In Africa, the role of audit committees has been evolving, especially with increasing economic integration and regulatory reforms across the continent. African nations are working towards strengthening their governance frameworks to improve transparency, accountability, and oversight, particularly in response to global trends like cybersecurity and ESG factors. The increasing reliance on digital infrastructure has led to rising concerns about cybersecurity risks in Africa (Alonge et al., 2024). As businesses and banks embrace technology, audit committees in the region are slowly taking more responsibility for overseeing cybersecurity frameworks. The King IV Report on Corporate Governance in South Africa, stresses the importance of governance on technology risks, including cybersecurity (Gwala, 2022). According to Daniels (2023), Nigeria has seen an uptick in regulatory reforms that require organizations to implement comprehensive cybersecurity risk management frameworks, which audit committees, must oversee.

As part of broader corporate governance reforms, there is increasing pressure for independent audit committees in Africa. Historically, many African companies have had closely-knit boards where management influence may overshadow independent oversight. However, reforms are pushing for greater independence. For instance, the OECD guidelines on corporate governance have influenced several African countries to improve audit committee independence, such as in Kenya and South Africa (Ahunwan, 2021).

In Kenya, there has been significant emphasis on improving governance structures within Kenyan companies, driven by both local and international pressure to improve transparency and accountability. This includes strengthening audit committees to ensure effective oversight of financial and operational risks. For instance, the Capital Markets Authority (CMA) in Kenya has set guidelines requiring companies listed on the Nairobi Securities Exchange (NSE) to have strong internal audit systems overseen by independent audit committees (Obade, 2021).

The audit committee's role in corporate governance is becoming more critical due to various reforms aimed at strengthening financial oversight and ensuring that companies are better

equipped to handle emerging risks like cybersecurity and compliance issues. As Kenya's banking sector and businesses move toward digital solutions, the role of audit committees in overseeing cybersecurity risks has become more pronounced. Kenya has seen a rising number of cyberattacks, prompting greater regulatory attention on how companies, especially banks, manage digital security (Oluoch, 2022). The Central Bank of Kenya (CBK) has emphasized the importance of cybersecurity in its governance frameworks for commercial banks, pushing audit committees to take a stronger role in overseeing cybersecurity policies (CBK, 2018). Additionally, the Computer Misuse and Cybercrimes Act (2018) in Kenya requires organizations to develop robust cybersecurity strategies, and audit committees now have to ensure that these strategies are in place and actively managed.

Usman et al. (2024) investigated the role internal auditors play in cybersecurity risk assessment, Matemane et al. (2024) examined the moderating effect of board characteristics on the relationship between cybersecurity risk disclosures and company performance in South Africa, Alodat et al. (2024) focused on how board characteristics influence cybersecurity disclosure (CSD), Elsayed et al. (2024) focused on the effect of cybersecurity disclosure on bank performance and the moderating effect of corporate governance while Al-Yasari and Saada (2024) assessed how the audit committees influence cybersecurity risks in banks in Iraq. Across the studies, there is a noticeable lack of focus on the moderating role of audit committee characteristics in the relationship between cybersecurity culture and financial performance in commercial banks. This study assessed the moderating effect of audit committee characteristics on the relationship between cybersecurity culture and the financial performance of commercial banks in Kenya.

In the context of the study, the expertise and independence of the audit committee were adopted as key characteristics. Both characteristics are critical in ensuring effective governance and oversight, especially when it comes to addressing the complex and evolving risks associated with cybersecurity. The landscape of cyber threats is continuously evolving, with increasingly sophisticated attacks targeting financial systems. Audit committee members with expertise in cybersecurity can identify vulnerabilities and provide valuable insights into how banks can better secure their operations, thus preventing financial loss and reputational damage and ensuring smooth business operations. An audit committee with members possessing technical and financial expertise is more likely to make informed decisions regarding the integration of cybersecurity measures into the broader risk management framework. For banks, where the stakes in managing financial risk, compliance, and cybersecurity are high, an independent audit

committee ensures that the decisions made are in the best interests of stakeholders, particularly shareholders, customers, and regulatory authorities. Independent members are more likely to prioritize the long-term health and security of the bank, ensuring that the bank's cybersecurity policies are not influenced by short-term management goals or internal politics.

1.1.3 Financial Performance

Financial performance refers to the measure of a company's profitability, efficiency, and overall financial health over a given period (Kyere & Ausloos, 2021). According to Inamdar, (2024) financial performance reflects how well a bank or financial institution is able to generate profits and sustain its operations while effectively managing its financial resources. Financial performance is typically evaluated using financial metrics and ratios that allow stakeholders, including investors, regulators, and managers, to assess the bank's ability to create value for its shareholders, meet financial obligations, and achieve its strategic objectives (Arora, 2022).

Globally, organizations focus on a mix of financial metrics to measure their performance. Common financial indicators such as profit margins, Return On Assets (ROA), Return On Equity (ROE), and Earnings Before Interest And Taxes (EBIT) are widely used (Vavrek et al., 2021). In the banking sector, the CAMEL (Capital adequacy, Asset quality, Management quality, Earnings, and Liquidity) model is primarily employed by bank regulators**,** supervisory authorities**,** and financial institutions to ensure the stability and soundness of banks (Haralayya & Aithal, 2021). The model provides a standard approach for assessing the core financial health of a bank and helps prevent financial crises by identifying areas of weakness before they escalate. While financial measures are critical for assessing the overall performance of banks, non-financial measures are equally important in providing a comprehensive view of a bank's long-term viability, customer satisfaction, and internal operational effectiveness (Omran et al., 2021).

In the banking sector, the use of financial metrics has been dominant; however, non-financial performance indicators have gained increasing prominence as banks face heightened competition, regulatory pressures, and the need to adapt to technological advancements. According to a McKinsey & Company report (2021), 72% of global businesses prioritize financial and operational performance metrics, but companies are increasingly incorporating non-financial factors like employee engagement and sustainability into their performance assessment. These additional dimensions are increasingly seen as important drivers of sustained organizational success.

In Europe, businesses are increasingly focusing on Environmental, Social, and Governance (ESG) metrics, which measure a company's impact on the environment, its social responsibility efforts, and its governance practices (Dmuchowski et al., 2023). The European Environment Agency (2024) has reported that more than 80% of large companies in the EU now track some form of ESG-related metrics, reflecting the growing importance of these factors in regional performance assessments.

In North America, especially in the United States, performance metrics have historically relied heavily on financial outcomes. However, with the rise of digital transformation, many companies now incorporate operational efficiency, digital adoption rates, and customer-centric measures such as Customer Lifetime Value (CLV) to gauge performance. According to Deloitte's (2020) survey, 63% of North American businesses now incorporate digital transformation metrics, including cybersecurity resilience, into their performance measurement systems.

In Africa, the regional focus on organizational performance is still evolving, largely due to economic challenges and rapid digital adoption. However, there is a significant increase in the use of performance metrics tied to financial health, operational efficiency, and the ability to adapt to technological shifts. According to the African Development Bank (2020), 60% of African businesses began incorporating digital technologies into their performance management systems. However, there is still a lack of comprehensive regional frameworks that adequately address both financial and non-financial performance indicators.

In Kenya, organizational performance in the context of commercial banks is measured through a combination of financial indicators, customer satisfaction, regulatory compliance, and technological adaptation (Kori et al., 2020). Commercial banks, being critical to the financial ecosystem, are held to high-performance standards, especially given the increasing focus on financial inclusion and digital banking. Similar to global practices, financial measures such as return on equity (ROE), return on assets (ROA), and loan growth are standard measures of success. In Kenya, commercial banks have consistently been evaluated based on their ability to maintain strong profitability and liquidity while balancing risks in a volatile market (Kirimi et al., 2022).

Past studies primarily focused on organizational financial and employee performance in diverse contexts, such as software development firms in Iran (Roustapisheh & Yazdizadeh, 2022), hospitals in Abuja, Nigeria (Mukaila et al., 2022), church-owned schools in Kenya (Karanja et

al., 2020), and state corporations in Kenya (Obogi & Kiarie, 2019). However, this study addresses a contextual gap by focusing specifically on the financial performance within the banking sector in Kenya, a critical aspect of economic development. This gap is particularly significant given the distinctive PESTEL (Political, Economic, Social, Technological, Environmental, and Legal) factors that influence the financial sector in Kenya. These include local economic conditions, government regulations, technological infrastructure, and legal frameworks, all of which shape the performance and strategies of Kenyan banks. Thus, the banking context in Kenya presents unique challenges and opportunities that have not been fully explored in previous studies.

Previous studies have predominantly relied on either secondary data or qualitative methods. For example, Kweon et al. (2021) explored cybersecurity incidents, Obogi & Kiarie (2019) focused on project performance using secondary data, Alzahrani and Seth (2021) on the performance of information security management among SMEs in the United Kingdom, Hovav et al. (2023) examined how security policies and cyber regulations affect organizational outcomes and Matemane et al. (2024) focused on examining the moderating effect of board characteristics on the relationship between cybersecurity risk disclosures and company performance. However, this study combined both secondary and primary data. Primary data collection involved direct responses from key stakeholders through surveys, providing real-time insights into the application of cybersecurity practices, management support, and training. Secondary data was used to analyze historical and financial records, providing a comprehensive view of how these factors influence financial performance. The combined methodological approach fills the gap of relying on just one type of data, allowing the study to provide more accurate and multidimensional insights.

Many of the past studies focused on organizational or employee performance (e.g., employee performance in hospitals by Mukaila et al. (2022)), cybersecurity incidents (Kweon et al., 2021), or project performance (Obogi & Kiarie, 2019), but none have conceptually explored the relationship between top management support, cybersecurity culture and financial performance in the banking industry. The inclusion of cybersecurity culture as a variable, alongside top management support, information security policies, and training, is a conceptual gap that the proposed study fills. These elements, which are particularly pertinent to the financial sector, have not been explored in the context of Tier II and Tier III banks in Kenya.

The financial performance was assessed through Return on Assets. The study adopted Return on Assets (ROA) as the measure of financial performance due to its direct reflection of how

efficiently the bank uses its assets to generate profit. This profitability ratio is particularly relevant when examining the impact of cybersecurity culture, as implementing effective cybersecurity measures can significantly reduce financial losses from cyber incidents and increase the bank's ability to utilize its assets effectively. By focusing on ROA, the study provides a clear understanding of how improvements in cybersecurity culture influence the financial performance of Kenyan commercial banks.

1.1.4 Commercial Banks in Kenya

The Central Bank of Kenya (CBK) regulates the banking sector in Kenya by ensuring that financial institutions comply with laws and regulations designed to safeguard the integrity and stability of the financial system. During the year ended June 30, 2024, the Kenyan banking sector consisted of 38 commercial banks (CBK, 2024). The Central Bank of Kenya (CBK) has established a categorization system for commercial banks based on their financial health, capital base, and operational scale. This classification system helps in evaluating the stability and strength of banks and allows regulators, investors, and consumers to understand the relative standing of each bank in the sector. The system divides banks into three tiers: Tier I, Tier II, and Tier III. The primary criteria for categorizing banks include the size of their assets, capital adequacy, and financial performance. There are 9 Tier 1 banks, 8 Tier II banks and 21 tier III banks (CBK, 2024).

Savings and checking accounts, loans, and other services like wealth management, foreign exchange, and mobile banking are amongst the wide array of financial services offered by commercial banks in Kenya. These banks are critical in the financial ecosystem, not only by offering essential services to individuals and businesses but also by contributing significantly to the country's economy (CBK, 2022).

The banking sector in Kenya plays a crucial role in the country's economic development and societal welfare. The banking sector provides the financial resources needed for investment in various sectors of the economy, including agriculture, manufacturing, and services. In 2023, the sector contributed approximately 5.1% of Kenya's GDP (Central Bank of Kenya, 2024). Kenya's banking sector compared to many other African countries, is well-developed with a large number of commercial banks, financial institutions, and microfinance institutions. The sector has seen notable transformations over the years, especially with the adoption of mobile banking and financial technology (FinTech) (Adhing'a & Gatauwa, 2023). Despite the significant advancements, commercial banks in Kenya face several challenges. The rise of non-

performing loans continues to be a challenge for Kenyan banks. While regulations in Kenya are designed to stabilize the banking sector, they can also create pressure on banks. The interest rate cap introduced in 2016, although repealed in 2019, had limited the profitability of banks (Ngaruiya et al., 2022). New regulations, particularly regarding mobile money and data privacy, continue to impact the way banks operate.

As commercial banks expand their digital services (e.g., mobile banking, online platforms), it becomes even more critical to embed a culture of security at all levels of the organization to safeguard financial data and customer trust. The cybersecurity culture of a bank can significantly influence its financial performance. Banks with a robust cybersecurity culture are less likely to face costly breaches, which can result in financial losses, regulatory fines, and reputational damage. The study focused on all the banks. The poor financial performance of the Tier II and Tier III banks compared to the Tier I banks justifies the need to explore how cybersecurity culture influences their financial performance. These banks are particularly vulnerable to cybersecurity risks due to their limited resources, yet they also have significant room for growth and improvement in this area. By investigating the link between cybersecurity culture and financial performance in these banks, the study may provide valuable insights into how even smaller, resource-constrained banks can improve their financial outcomes through cost-effective cybersecurity measures.

1.2 Statement of the Problem

In Kenya's banking sector, especially for Tier II and III banks, the increasing number of cyber threats poses a substantial risk to financial stability. The Central Bank of Kenya (CBK) has raised concerns about the inadequate cybersecurity preparedness of these banks, which are more vulnerable due to limited resources and outdated systems, making them prime targets for cybercriminals (CBK, 2023). This lack of cybersecurity integration threatens their financial performance, especially when compared to more secure Tier I banks. According to CBK (2023), in December 2023, Tier 2 banks experienced a decrease in market share to 15.0%, down from 16.3% in 2022. Tier 3 banks saw an even more dramatic decrease to 8.4% from 8.6% in the previous year. Moreover, a comparison of Profit Before Tax (PBT) highlights the stark contrast in profitability, with large banks showing significantly higher PBT margins than Tier II and III banks. This discrepancy is indicative of the substantial challenges these smaller banks face in maintaining financial stability. This crisis may be compounded by a failure to implement effective cybersecurity measures that align with the growing demands of the digital banking environment. Thus, there is an urgent need to understand how aspects of cybersecurity

culture and top management support affect the financial performance of Kenya's commercial banks.

Roustapisheh and Yazdizadeh (2022) assessed the effects of top management support on organizational performance and found that top management's assistance has an indirect, positive, and significant impact on performance of organizations. Alzahrani and Seth (2021) on the impact of security organizational methods on the performance of information security management among SMEs in the United Kingdom found information security performance is greatly impacted by security education and security training. Kong et al. (2023) investigation focused on information security operations' effect on organizational performance in the securities industry in Korea, Fagbule (2023) examined training effectiveness in SMEs in England and that content quality and delivery methods as key factors, De Jager et al. (2023) investigated the gap in cybersecurity skills in South Africa and identified the lack of skills and resources as a significant barrier to cybersecurity effectiveness. Locally, Okubo et al. (2024) on the influence of the management of information security on the performance of the Ministry of Roads and Transport found that information security management is statistically significant in explaining the supply chain performance. Ropem (2024) found that thorough training initiatives improved employees' cybersecurity awareness in Kenyan corporate environments and Okubo et al. (2024) examined how information security management relates to performance in Kenya's Ministry of Roads and Transport. While several studies have explored the individual factors influencing cybersecurity in various sectors, a significant gap remains in understanding how these factors collectively contribute to financial performance in the context of Kenyan commercial banks. This study sought to fill these gaps by exploring how key components of cybersecurity culture, moderated by audit committee characteristics, influence the financial performance of commercial banks in Kenya.

1.3 Research Objectives

1.3.1 General Objective

This study's general objective was to determine the perceived effect of cybersecurity culture on financial performance of Kenyan Commercial Banks: Moderated by Audit Committee Characteristics.

1.3.2 Specific Objectives

1. To determine the effect of top management support on the financial performance of commercial banks in Kenya.

2. To examine the effect of information security policy on the financial performance of commercial banks in Kenya
3. To investigate the effect of cyber security training on the financial performance of commercial banks in Kenya.
4. To assess the moderating effect of audit committee characteristics on the relationship between cybersecurity culture and financial performance of commercial banks in Kenya.

1.4 Research Questions

1. What is the effect of top management support on the financial performance of commercial banks in Kenya?
2. How does information security policy influence the financial performance of commercial banks in Kenya?
3. To what extent does cybersecurity training influence the financial performance of commercial banks in Kenya?
4. What is the moderating effect of audit committee characteristics on the relationship between cybersecurity culture and the financial performance of commercial banks in Kenya?

1.5 Scope of the Study

The study focused on cybersecurity culture and its effect on the financial performance of commercial banks in Kenya, moderated by Audit Committee Characteristics. Three independent variables, top management support, information security policy and cyber security training were studied and how they impact the financial performance of commercial banks in Kenya. The study was conducted in the 38 commercial banks headquarters in Nairobi. The study was conducted between the months of March to April 2025. The study used a sample of 3 individuals per bank, selected based on their role and knowledge of the relevant issues. Thus, the total sample size was 114 participants.

1.6 Significance of the Study

1.6.1 Policy Makers

The findings of this study may be used to advise policymakers and regulators in coming up with regulations, policy frameworks, and guidelines aimed at strengthening cybersecurity

practices across the Kenyan banking sector. By identifying key factors that influence cybersecurity culture, the study can contribute to developing robust policies which can enhance the resilience and security of financial institutions.

1.6.2 Management of Commercial banks

Bank executives, managers, and decision makers can use the study findings to embed cybersecurity culture initiatives as part of their strategies to drive financial performance and remain competitive. By integrating a strong cybersecurity culture into organizational frameworks, commercial banks can improve their financial performance and operational effectiveness, reduce risks, and ensure the safety of their systems and customer data.

1.6.3 Academia

This study may contribute to the body of knowledge and serve as the basis for future research by academicians. It may provide a foundation for scholars to explore further the link between cybersecurity culture and financial performance, potentially leading to the development of new theories and frameworks in this area.

1.7 Chapter Summary

This chapter has introduced the study by providing a detailed background of the study under the sections of cyber security culture, financial performance, audit committee characteristics and the interplay between cyber security culture and financial performance. The chapter also provides the statement of the problem, the objectives, the research questions that the study seeks to answer, and the scope and significance of the study. The next chapter presents the literature review.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents a critical review of literature that is related to cybersecurity culture and its impact on financial performance. The chapter is organized into the following sections: theoretical literature, empirical review based on the research objectives, research gaps identified and the conceptual framework.

2.2 Theoretical Foundation

The study was anchored on the institutional theory, the Resource-Based View (RBV) and the Agency Theory. A single theory may not adequately capture the multi-dimensional nature of the proposed research. By integrating these three theories, the study adopts a multi-theory approach, allowing for a more comprehensive understanding where each of these theories offers a unique perspective to help explain how various elements such as top management support, information security policy, cybersecurity training, and audit committee characteristics affect the performance of these banks.

2.2.1 Institutional Theory

Institutional Theory was primarily developed by sociologists John W. Meyer and Brian Rowan in the early 1970s. Their seminal work, which laid the foundation for Institutional Theory, focused on how organizations conform to societal expectations and institutional pressures, even when such conformity does not directly contribute to their operational efficiency. Meyer and Rowan's work argued that organizations often adopt structures, policies, and practices that conform to the institutionalized norms and values of the environment in which they operate, to gain legitimacy, resources, and survival, even if these practices may not be the most effective or efficient (Meyer & Rowan, 1977).

Institutional Theory primarily focuses on the way organizations are influenced by external pressures such as norms, regulations, and cultural expectations within their environment. It suggests that organizations are not solely driven by market competition but are also shaped by the institutional frameworks within which they operate (Peters, 2022). These frameworks can include government policies, industry standards, regulatory bodies, and societal expectations. Institutions, in this context, exert significant influence on organizational behavior, as

organizations strive to conform to these external pressures to gain legitimacy, maintain resources, and ensure long-term survival.

One major critique is that it overemphasizes the role of external pressures, such as norms, regulations, and social expectations, in shaping organizational behavior, often at the expense of ignoring the internal dynamics and strategic decisions within the organization. Critics argue that the theory tends to present organizations as passive entities that simply adapt to their environment, without considering their agency and capacity for active change or innovation (Suddaby, 2010). Furthermore, the theory has been criticized for its lack of clear mechanisms or processes through which institutional pressures influence organizations, making it challenging to apply in practical, real-world scenarios. Additionally, critics point out that Institutional Theory does not adequately address how organizations can effectively balance the tension between conformity to institutional pressures and the need for differentiation or competitive advantage (Willmott, 2015).

Institutional Theory anchors the examination of how external institutional forces influence commercial banks' performance in Kenya in this study, particularly regarding cybersecurity practices. In Kenya, financial institutions, including commercial banks, operate in a highly regulated environment, with institutions such as the Central Bank of Kenya (CBK) playing a critical role in setting policies, standards, and guidelines for operations, including cybersecurity practices. The Kenyan government also enforces regulations related to data protection, fraud prevention, and cybersecurity, which compel banks to adopt specific security policies and ensure compliance.

This theory supports the idea that top management support (objective 1) and the information security policy (objective 2) are influenced by the external institutional environment. Top management may emphasize cybersecurity practices to align with institutional pressures and regulatory requirements, while information security policies are often shaped by the need to meet these external institutional mandates. Therefore, Institutional Theory helps to explain how external pressures, such as regulatory requirements or industry standards, impact how commercial banks in Kenya adopt and implement cybersecurity measures to ensure compliance and enhance performance.

2.2.2 The Resource-Based View (RBV)

The Resource-Based View (RBV) theory of the firm is primarily associated with the work of Birger Wernerfelt(1984), Jay Barney (1991), and Edith Penrose (1959). The Resource-Based

View (RBV) theory, in strategic management, is a prominent framework that emphasizes the internal resources and capabilities of an organization as the primary sources of competitive advantage. Scholars such as Jay Barney developed the RBV theory in the 1980s, which shifts the focus from external market factors to organizations' internal assets and competencies. The central premise of RBV is that firms can achieve sustained competitive advantage through the unique combination of resources they control, and these resources must meet specific criteria to provide that advantage (Lubis, 2022).

In RBV, resources are considered the assets and inputs that organizations use to produce goods or services. Resources can be tangible (e.g., financial capital, physical assets, technology) or intangible (e.g., brand reputation, intellectual property, organizational culture, or employee skills). On the other hand, capabilities are the firm's ability to effectively utilize its resources (Lubis, 2022). For example, a firm's capabilities might include its managerial expertise, innovation processes, or customer service systems. The VRIO (Valuable, Rare, Imitable, Organized to Capture Value) framework is a tool used within the RBV to assess whether a resource or capability can provide a sustained competitive advantage. One of the fundamental ideas in RBV is the notion of sustained competitive advantage. The RBV asserts that resources that are valuable, rare, difficult to imitate, and well-organized within the firm can lead to long-term success. These can include proprietary technology, unique customer relationships, or distinctive organizational cultures that are challenging to competitors to replicate. A further extension of the RBV is the concept of dynamic capabilities. This concept focuses on the ability of a firm to respond to changes in the external environment by adapting and reconfiguring its resources and capabilities (Kero & Bogale, 2023).

Despite its widespread use, the Resource-Based View has faced criticism on several fronts. Ariwibowo et al. (2021) argue that the RBV overemphasizes the role of internal resources while downplaying the importance of external aspects, such as market conditions, trends in the industry, or competition. Another challenge with RBV is that it can be difficult to identify which resources are truly valuable, rare, and inimitable. For example, a company might have a wide range of resources, but not all of them contribute equally to its competitive advantage. While the RBV focuses on leveraging internal resources, it focuses less on how organizations can adapt to shifting external environments. Within industries where rapid technological change or shifting customer preferences occur, organizations need to be able to respond quickly, which may not always be aligned with the RBV's emphasis on sustaining existing resources (Zahra, 2021).

In the Kenyan context, where the banking sector is rapidly evolving and digitizing, the RBV is particularly relevant. With increasing cyber threats, Kenyan banks that invest in cybersecurity infrastructure and cultivate a strong cybersecurity culture will not only comply with regulations but also gain a competitive edge in an industry that is highly dependent on customer trust and security. This theory helps to explain how the interplay between top management support, information security policies, cyber security training, and the overall cyber security culture can significantly enhance the performance of commercial banks operating in Kenya.

In relation to this study's objectives, RBV supports examining how resources (cybersecurity culture, top management support, and policies) contribute to the performance of banks. The theory helps clarify the connection between these resources and the organizational outcomes (financial performance) as it relates to the first three specific objectives: 1) the effect of top management support, 2) the effect of information security policy, and 3) the effect of cybersecurity training. Additionally, it links to the fourth objective, which assesses the moderating effect of audit committee characteristics on the relationship between cybersecurity culture and financial performance, showing that effective governance structures can enhance the value of cybersecurity resources. Thus, RBV underpins the idea that these resources, when effectively leveraged, contribute to organizational success in Kenya's banking sector.

2.2.3 Agency Theory

Michael Jensen and William Meckling developed the agency theory in 1976, which focused on the principal-agent relationship, where a principal (e.g., shareholder) delegates decision-making to an agent (e.g., manager). The theory suggests that conflicts of interest may arise due to information asymmetry, where agents often have more detailed knowledge and may act in ways that benefit themselves rather than the principal (Raimo et al., 2021). This can lead to inefficiencies and suboptimal outcomes. The theory proposes mechanisms like performance-based incentives (e.g., bonuses, stock options) and strong corporate governance, including an independent audit committee and regular audits to mitigate these issues.

Agency theory also highlights potential conflicts of interest, where agents may pursue personal goals, such as higher salaries or job security, that diverge from the principal's objectives, like maximizing shareholder value. To align these interests, performance incentives and effective governance mechanisms are suggested. However, critics argue that the theory overly assumes managers are purely self-interested and neglects the possibility of managers' actions being in the organization's best interests. It also overlooks the complexity of relationships in real-world

organizations, where multiple stakeholders and non-financial motivations influence decision-making (Ain et al., 2021).

Despite its widespread use, agency theory has been criticized for simplifying the dynamics between principals and agents. It tends to focus on financial incentives and short-term performance, potentially promoting risky decision-making and neglecting long-term sustainability. The theory also doesn't fully consider organizational culture and ethical behaviour's roles in shaping managerial actions. Agency theory is sometimes criticized for oversimplifying the relationships between principals and agents. In reality, these relationships are often more complex, with multiple stakeholders (employees, customers, suppliers) involved in decision-making, and agents may face conflicting incentives that the theory does not address easily (Davis et al., 2021).

In the Kenyan banking context, where trust and regulatory compliance are critical, agency theory becomes highly relevant. Banks must align the interests of their executives with the overarching goals of ensuring financial stability and security, particularly in relation to cybersecurity practices. For example, top management (agents) should prioritize establishing a strong cybersecurity culture that aligns with the bank's overall objectives of data security and customer trust, ensuring that the owners' (principals') interests are protected. The involvement of the audit committee, as highlighted in the study, serves as a monitoring mechanism to ensure that management actions, particularly those related to cybersecurity culture, are aligned with the interests of both the owners and the broader stakeholders.

Concerning the study objectives, agency theory supports the examination of the moderating effect of audit committee characteristics on the correlation between cybersecurity culture and financial performance (Objective 4). The theory suggests that audit committees, as part of governance structures, have a critical role in monitoring and guiding the behavior of management (agents) to ensure that cybersecurity policies, training, and resources are effectively utilized to improve banks' financial performance.

2.3 Empirical Literature Review

A systematic literature search was conducted to find the various constructs of cybersecurity culture and its impact on financial performance. The searches were conducted in Google Scholar and databases such as Science Direct, JStor to identify relevant research papers. The aspects cybersecurity culture were selected based on Alnatheer's (2014) conceptual model and recurring themes in the literature that emphasize their critical role in shaping an organization's

cybersecurity readiness and response. However, the review also reveals notable gaps; for instance, few studies have examined these elements within the context of financial institutions in developing economies, particularly in Kenya.

2.3.1 Top Management Support and Financial Performance

Top Management Support refers to the active involvement and commitment of senior leaders (such as CEOs, CFOs, and other high-level executives) in fostering and promoting a strong cybersecurity culture within an organization. This includes providing necessary resources, setting strategic priorities, and demonstrating through their actions the importance of cybersecurity (Obogi & Kiarie, 2019).

Roustapisheh and Yazdizadeh (2022), Mukaila et al. (2022), and Gale et al. (2022) examined management support and its influence on organizational performance. However, their focus was primarily on general performance in software firms, hospitals, and organizational leadership rather than the specialized impact on financial performance. These studies did not explicitly address how top management support relates to financial performance. Smaili et al. (2023) and Obogi and Kiarie (2019) also explored management's role in organizational performance but extended the focus to cybersecurity disclosures and project performance. While these studies touched on board effectiveness and management support, neither focused on top management support and its direct link to financial performance in banks—a vital gap considering the growing role of cybersecurity in the financial sector. Karanja et al. (2020) examined senior management commitment and school performance but not financial performance. The focus on non-financial sectors (education) limits this study's applicability to banks, where cybersecurity is critical.

Roustapisheh and Yazdizadeh (2022) conducted their study in Iran within software development firms, a sector with different technological, regulatory, and cyber risk dynamics than the banking sector in Kenya. The Kenyan tier II and III banks face unique cybersecurity challenges, such as limited resources, which were not addressed in studies conducted in more technologically developed settings like Iran. Mukaila et al. (2022) conducted their study in Nigerian hospitals, focusing on employee performance rather than organizational cybersecurity performance. Their findings, though valuable for understanding general management support, do not translate easily to Kenya's Tier II and III commercial banks, where the threat of cybercrime and its impact on financial performance is much more pronounced. Gale et al. (2022) focused on directors' involvement in cybersecurity in various organizations, yet this

study lacks a specific focus on the banking sector. The findings about the external pressure from regulations and the involvement of experts may be more applicable to large firms, like Tier I banks, rather than Tier II and III banks, which face different challenges, such as outdated systems and a lack of resources for robust cybersecurity measures.

Roustapisheh and Yazdizadeh (2022), Mukaila et al. (2022) and Gale et al. (2022) used quantitative methods. However, neither study used mixed methods. This qualitative approach limits the ability to assess direct causal relationships. Smaili et al. (2023) used secondary data from Canadian listed companies, which lacks the immediacy and relevance of primary data in understanding the cybersecurity needs of Tier II and III Kenyan banks. Obogi and Kiarie (2019) and Karanja et al. (2020) employed descriptive survey designs with questionnaires to gather data from relatively few respondents. However, while these methods are useful for broad insights, they lack the depth needed to explore the relationships between cybersecurity culture, management support, and financial performance, particularly in Tier II and III banks that face specific cybersecurity challenges.

While Roustapisheh and Yazdizadeh (2022) and Gale et al. (2022) emphasize the positive relationship between management support and organizational performance, they fail to consider cybersecurity culture, which could be the missing link in explaining performance outcomes, especially in a cybersecurity-intensive sector like banking. In contrast, Smaili et al. (2023) found that board effectiveness positively impacts cybersecurity disclosures but did not explore its effect on financial performance, which could create conflicting findings regarding the direct link between cybersecurity and financial performance in the banking sector. Karanja et al. (2020) found that senior management commitment significantly influences organizational performance but did not account for the critical role of cybersecurity in today's organizational success. This oversight may explain why their findings differ from those in banks, where cybersecurity culture is paramount to financial performance. Additionally, the study's focus on schools rather than financial institutions creates a gap in understanding the role of management support in cybersecurity-related performance.

2.3.2 Information Security Policy and Financial Performance

Information Security Policy refers to the set of guidelines, principles, and practices established by an organization to protect its information systems, networks, and data from unauthorized access, disclosure, alteration, and destruction. The policy outlines how the bank manages and safeguards data and IT resources (Alraja et al., 2023).

Kong et al. (2023) investigation focused on information security operations' effect on organizational performance in the securities industry in Korea. Their study emphasizes organizational performance and transaction stability in the financial sector, but it does not explicitly address Information security policy within organizations and impact on fiancnial performance. Additionally, their findings focus more on transaction stability than on specific financial performance indicators, which leaves a gap in understanding how these policies relate to overall financial success in industries like banking. Alzahrani and Seth (2021) studied how organizational security practices affect information security management performance in the small and medium-sized enterprises (SMEs) in UK. The focus on security education, training, and knowledge exchange shows how specific organizational practices influence the performance of information security. However, this study is limited by its focus on SMEs in the UK, which may have different cybersecurity challenges and performance metrics compared to Tier II and III commercial banks in Kenya.

Hovav et al. (2023) focused on how cyber regulations and security policies affect knowledge management (KM) processes and their relationship with organizational effectiveness and strategic performance. While this study introduces knowledge management as an intermediary between security policies and performance, it does not explore how information security practices directly affect financial performance, which is the core concern of this proposed study. Okubo et al. (2024) examined how information security management relates to performance in Kenya's Ministry of Roads and Transport. The findings are more relevant for government institutions rather than commercial banks, leaving a gap in understanding how information security policies impact the financial performance of Kenya's Tier II and III commercial banks.

Alzahrani and Seth (2021) studied SMEs in the UK, which face a distinct set of cybersecurity challenges compared to Kenyan banks. Kong et al. (2023) focused on the Korean securities industry, a well-established financial sector. While the findings are relevant for financial performance, they may not fully apply to commercial banks operating in Tier II and III in Kenya, where cybersecurity threats and technological capabilities differ substantially. Kubo et al. (2024) focused on the Ministry of Roads and Transport in Kenya, an entirely different context from the banking sector. The applicability of their research's findings to Tier II and III commercial banks is limited by this contextual gap as these banks face different types of cybersecurity threats and have distinct organizational goals related to financial performance.

The methodological differences across the studies, such as the use of survey methods versus qualitative interviews or secondary data, contribute to the conflicting findings, especially regarding the role of information security policies. This highlights the need for further research in exploring the influence of information security policies on financial performance in Kenyan banks, using a mixed-methods approach that will capture both the quantitative effect and the qualitative nuances of cybersecurity culture.

2.3.3 Cyber Security Training and Financial Performance

Cybersecurity Training refers to the educational programs designed to enhance employees' awareness and understanding of cybersecurity threats, practices, and tools. It includes training on how to identify and prevent cyber threats such as phishing, malware, and social engineering attacks (Fagbule, 2023). This training may cover best practices for protecting sensitive data, safe use of corporate it resources and how to recognize potential cyber threats, security protocols for password management and secure communication.

Al-Alawi & Al-Bassam (2019) emphasized the importance of staff training in raising awareness about cyber threats. Their focus was primarily on how well-trained and aware staff contribute to organizational security, but it lacks an exploration of how training directly impacts financial outcomes. Kweon et al. (2021) took a more quantitative approach to explore the relationship between cybersecurity training and the incidence of cyberattacks in South Korea. Their study demonstrates a negative correlation between cybersecurity training and the frequency of cybersecurity incidents. This study highlights the effectiveness of training in reducing cyber threats, but it doesn't address the broader organizational impact of fewer incidents, such as improved performance or cost reduction related to incident mitigation. Fagbule (2023) used a qualitative methodology to examine training effectiveness in SMEs in England. This study focused on content quality and delivery methods as key factors affecting employee engagement with cybersecurity training. However, it does not link training outcomes directly to financial performance. Instead, it highlights that poorly designed training leads to disengaged employees, indicating a failure to align training with organizational goals.

De Jager et al. (2023) investigated the gap in cybersecurity skills in South Africa, focusing on the challenges and needs in developing cybersecurity expertise. The study is centered on resources and investment in developing a skilled cybersecurity workforce. While it identifies the lack of skills and resources as a significant barrier to cybersecurity effectiveness, it does not directly connect these findings to financial performance outcomes, such as improved

security measures or reduced risk exposure. Ropem (2024) explored the impact of cybersecurity training programs on employee behaviour in Kenya. The research focused on how training initiatives can improve employees' cybersecurity awareness and adherence to practices, ultimately fostering a sense of responsibility. However, it does not explore the wider organizational effects or financial implications of improved employee behaviour, such as reduced risk or increased productivity.

In addition, Kweon et al. (2021) conducted their research in South Korea, a country with advanced technological infrastructure and cybersecurity capabilities, which could make their findings less applicable to organizations in regions with different levels of technological maturity, such as Kenya. Fagbule (2023) studied SMEs in England, which are smaller than larger organizations. The training challenges in SMEs may differ significantly from larger companies, and the findings are not directly applicable to corporate environments or larger organizations, especially in developing countries such as Kenya. De Jager et al. (2023) focused on South Africa's IT professionals, highlighting a cybersecurity skills gap that is tied to resource limitations and underfunding. This study is highly specific to the South African context and may not fully apply to other countries, particularly those with different cybersecurity funding and skill development policies, such as Kenya.

2.3.4 Moderating effect of Audit Committee Characteristics on the relationship between cybersecurity culture and Financial performance

Audit Committee Characteristics refer to the attributes of the audit committee within an organization that influence its effectiveness in overseeing financial and operational controls, including cybersecurity risk management. These characteristics may include independence, expertise, size and composition, meetings frequency and commitment to cybersecurity.The audit committee's characteristics can influence how well cybersecurity risks are monitored, reported, and managed (Usman et al., 2024).

Usman et al. (2024) explored the role of internal auditors in assessing cybersecurity risks within financial organizations, Alodat et al. (2024) focused on the board of directors' characteristics in influencing cybersecurity disclosures while Al-Yasari and Saada (2024) explored the board characteristics' influence on cybersecurity threats in Iraqi banks. These studies emphasize that audit committee characteristics, including professional ethics, skills competencies, and reward mechanisms, are critical in mitigating cybersecurity risks. However, the study does not examine the moderating role of audit committee characteristics directly on the relationship

between cybersecurity culture or top management and financial performance. Matemane et al. (2024) investigated how board characteristics (such as gender and ethnic diversity) moderate the relationship between cybersecurity risk disclosure and company performance. The findings suggest that diverse boards can improve how companies manage cybersecurity risks, leading to better company performance. This study directly examines the moderating effect of board characteristics, though it focuses on cybersecurity risk disclosure rather than cybersecurity culture, limiting the scope of understanding in terms of financial performance outcomes related to culture.

Matemane et al. (2024) studied companies in South Africa listed on the Johannesburg Stock Exchange (JSE), Alodat et al. (2024) focused on listed firms on the London Stock Exchange (LSE), Elsayed et al. (2024) looked at MENA-region banks, analyzing how cybersecurity disclosure and corporate governance affect bank performance while Al-Yasari and Saada (2024) focused on Iraqi banks, providing insights into cybersecurity risk management in developing economies. However, the studies span diverse regions (e.g., South Africa, MENA, Iraq), limiting generalizability across different geopolitical contexts. Further research is required to study the cross-border applicability of these findings.

Furthermore, Usman et al. (2024) employed a literature review methodology, Matemane et al. (2024) employed content analysis while Alodat et al. (2024) used an empirical approach with a large sample size from the LSE which lacked empirical testing of the moderating effects using robust, mixed-method approaches, combining qualitative insights with quantitative analyses to better understand the relationships between audit committees, cybersecurity culture, and financial performance.

2.4 Literature Gaps

The reviewed empirical studies have limitations in sample size**,** sector specificity, and research design (e.g., descriptive vs. causal studies). More robust sampling methods and analytical techniques like regression analysis and mixed methods are needed to establish the influence of cybersecurity culture on the financial performance of commercial banks in Kenya, moderated by audit committee characteristics. Some of the studies are conducted in different industries (securities, SMEs, government, and road transport) with different regulatory and operational structures, making them less applicable to the banking context in Kenya. Many of the studies, such as Gale et al. (2022) and Al-Yasari & Saada (2024), primarily focus on contexts outside of Kenya, such as Canadian and MENA regions, and often examine the relationship between

audit committee characteristics and cybersecurity from a disclosure or risk management perspective. These studies do not fully explore how audit committee characteristics moderate the relationship between cybersecurity culture and financial performance specifically in the Kenyan banking context. A summary of the literature review and research gaps is presented in Table 2.1.

Table 2.1: Summary of Knowledge Gaps

Author	Title	Methodology	Findings	Gaps
Roustapisheh and Yazdizadeh (2022)	Effects of top management support, technological skills, and capabilities on entrepreneurship and organizational performance.	Structural Equation Modeling. LISREL program	Top management's assistance has an indirect, significant, and positive impact on organizational entrepreneurship and performance.	This study focuses on software development firms in Iran, which is a different context compared to commercial banks in Kenya.
Mukaila et al. (2022)	The link between management support and employee performance in selected hospitals in Abuja, Nigeria	Survey method, structural equation modeling method	Management support for change has a positive and statistically significant impact on employee performance.	The study centers on employee performance as an outcome of management support, while financial performance in the banking sector encompasses a broader range of indicators

Alzahrani and Seth (2021).	The impact of security organizational methods on the performance of information security management among SMEs in the United Kingdom	The SPSS Amos 22 tool is used to evaluate the data using the structural equation model	Information security performance is greatly impacted by security education, security training, security visibility, and knowledge exchange	Conducted on small and medium-sized enterprises (SMEs) in the United Kingdom, which have different regulatory, financial, and operational dynamics compared to commercial banks in Kenya.
Okubo et al. (2024)	Influence of information security management on performance of Ministry of Roads and Transport in Kenya	Cross-sectional survey design	Information security management is statistically significant in explaining supply chain performance of Ministry of Roads and Transport in Kenya	The study focuses on the impact of information security management on supply chain performance, which is a narrower focus than the broad concept of financial performance

Kweon et al. (2021)	Relationship between cybersecurity training and the number of incidents of organizations in South Korea	Poisson regression approach	Security training and education have quantifiable positive relationship with minimizing the number of cybercrime incidents in businesses.	It focuses on incident reduction rather than linking training directly to financial performance indicators
Ropem (2024)	Impact of cybersecurity training programs on employee behavior in Kenyan corporate environments	Desk review methodology	Thorough training initiatives improved employees' cybersecurity awareness and adherence to standard practices	Uses a desk methodology based on previously published studies, which limits the ability to draw new empirical conclusions.
Usman et al. (2024)	Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations	Literature review approach	Internal auditors in cybersecurity risk assessments is influenced by professional ethics, personality traits, professional skills and competency	Literature review methodology limits the study's ability to generate primary data or empirical insights

Source: Researcher (2025).

2.5 Conceptual Framework

The relationship between this study's independent and dependent variables is illustrated in figure 2.3 below. The financial performance of commercial banks in Kenya is the dependent variable. The independent variables are top management support, information security policy and cybersecurity training. Audit committee characteristics is the moderating variable. Additionally, further constructs were adopted from Hasani et al. (2023) regarding the adoption of cybersecurity.

Management support, information security policies, cybersecurity training, and audit committee characteristics play a critical role in enhancing the financial performance of commercial banks. From the perspective of the Resource-Based View (RBV) theory, these elements are considered strategic internal resources that are valuable, rare, inimitable, and non-substitutable. In parallel, Institutional Theory explains the adoption of such practices as responses to external institutional pressures, including regulatory requirements, industry standards, and societal expectations. Furthermore, Agency Theory emphasizes the importance of governance mechanisms, such as audit committees, in mitigating agency conflicts between managers (agents) and shareholders (principals).

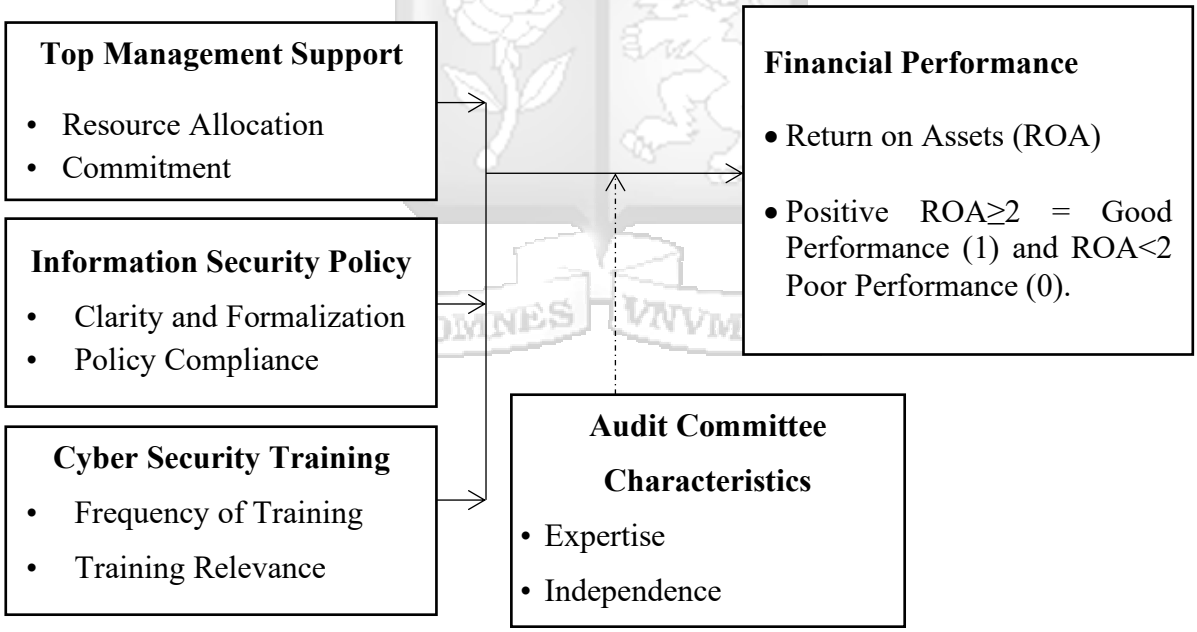

Figure 2.1: Conceptual Framework

Source; Researcher (2025)

2.6 Operationalization of variables

Several measures were adopted from existing literature to operationalize the variables identified in the conceptual framework as tabled below.

Table 2.2: Operationalization of variables

Variables	Variable definition	Indicators	Measures	Source of Measures
Top management support (TMS)	• Extent to which top management demonstrates commitment, involvement, and leadership in promoting cybersecurity efforts.	• Resource Allocation • Commitment	5-point Likert scale	Mukaila et al. (2022)
Information security policy	• Formal document that outlines the rules and guidelines for protecting an organization's information assets.	• Clarity and Formalization • Policy Compliance	5-point Likert scale	Hovav et al. (2023)
Cybersecurity training	• Programs designed to educate employees about best practices in cybersecurity and how to mitigate risks.	• Frequency of Training • Training Relevance	5-point Likert scale	(Al-Alawi & Al-Bassam, 2019; Kweon et al. (2021)

Variables	Variable definition	Indicators	Measures	Source of Measures
Audit committee characteristics	• Features of the audit committee such as expertise, independence, and involvement in overseeing cybersecurity.	• Expertise • Independence	5-point Likert scale	Usman et al. (2024)
Financial Performance	• The variable indicator was Return on Assets (ROA)	• Return on Assets (ROA) positive ROA = Good Performance (1) and negative ROA = Poor Performance (0)	• Continous	(Hasani et al., 2023)

2.7 Chapter Summary

This chapter has provided a review of relevant literature, focusing on the key concepts and theories that underpin the study, and the empirical research surrounding the relationship between cybersecurity culture and financial performance in commercial banks. Additionally, the chapter has presented the conceptual framework and the operationalization of the study variables.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research philosophy adopted, research design adopted, the study site, the survey population, sampling procedures, data sources, data collection tools/procedures, and data analysis that was applied in determining the impact of cybersecurity culture on financial performance of commercial banks in Kenya.

3.2 Research Philosophy

A system of assumptions and beliefs about the development of knowledge is defined as research philosophy (Saunders et al., 2023). Positivism focuses on objectivity and measurable data, typically using quantitative methods. Interpretivism emphasizes understanding subjective experiences and typically uses qualitative methods (Potrac et al., 2014). Realism believes in an objective reality but accepts that our perceptions mediate our understanding. Pragmatism is flexible and combines methods depending on the research question. Constructivism views knowledge as a social construct and typically uses qualitative approaches. Critical Theory seeks to challenge existing power structures and uses qualitative methods for social critique (Sobh & Perry, 2006).

This study adopted a positivist research philosophy where reality is characterized by stability with one being able to easily observe and describe it in an objective way. Positivism utilizes a scientific empirical method to make observations through approaches such as the structured questionnaire that this study adopted (Saunders et al., 2023). Further, positivism focuses on observable and measurable facts, with the researcher remaining neutral, detached and independent. The study thus sought to uncover generalizable patterns and relationships that can give insights into the influence of cybersecurity culture on financial performance of commercial banks in Kenya.

3.3 Research Design

The research design is a researcher's approach in answering the research question and meet the objectives of the study (Saunders et al., 2023). There are several research designs including descriptive which describe characteristics, behaviors, or conditions of a subject or phenomenon without manipulating variables, exploratory research design which investigate a problem or phenomenon that has not been extensively studied, to gain insights or generate hypotheses,

explanatory (causal) research design which determine the cause-and-effect relationships between variables, correlational research design which identify and measure the relationships between two or more variables, experimental research design which establish causal relationships by manipulating one or more independent variables and observing the effects on dependent variables (Abbott & McKinney, 2012).

In this study, the research design was a descriptive cross-sectional research design. A cross-sectional research design is one in which data is collected at a single point in time or over a very short period, typically using surveys or questionnaires. This design is used to examine relationships between variables or to assess the current state of affairs within a specific population at one moment. It helps researchers gather data from a sample of the population to make inferences or generalizations about the whole population. The descriptive cross-sectional aspect enabled the researcher to gather data from multiple banks at a single point in time, allowing for an analysis of relationships between cybersecurity culture and financial performance, as moderated by audit committee characteristics, without requiring long-term data collection.

Along with the questionnaire, an independent collection of financial performance data was done. This design allowed the research to determine the existing relationships between the financial performance of commercial banks in Kenya, which is the dependent variable, and top management support, information security policy, and cyber security training which are independent variables, as well as how audit committee characteristics moderate this relationship.

3.4 Target Population

The 38 commercial banks operating in Kenya as per the CBK, (2024) report, were the target population. These banks were selected due to their significant potential vulnerability to cybersecurity threats.

3.5 Sampling Design

3.5.1 Sampling Frame

The sampling units consisted of managers or department heads within the 38 selected banks. These individuals were expected to have detailed knowledge about the bank's cybersecurity culture, the financial performance of the institution, and the role of the audit committee. The

participants included Chief Information Security Officer (CISO) / Head of IT Department / Head of Internal Audit / Audit Manager, Chief Financial Officer (CFO) or Finance Manager.

3.5.2 Sample Size

The study used a sample of 3 individuals per bank, selected based on their role and knowledge of the relevant issues. Thus, the total sample size was 114 participants.

3.5.3 Sampling Techniques and Procedures

Given the nature of the study, a judgmental sampling approach was adopted, which was appropriate as the researcher needed to select a specific subset of the population with expert knowledge or key insights into the research topic. The focus was on selecting individuals who were directly involved in cybersecurity decision-making, financial performance monitoring, and audit committee activities.

3.6 Data Collection Methods

The study used a structured questionnaire tool to collect primary data. The research instrument was developed based on insights drawn from both existing empirical literature and relevant theoretical frameworks. The survey was designed using a 5-point Likert scale ranging from strongly disagree, disagree, neither agree nor disagree, agree, and strongly agree with assigned values from 1 to 5. Additionally, the study respondents were requested to provide additional demographic information about their banks. Section one was on demographic data while section two collected data on cybersecurity culture and audit committee characteristics. The survey questionnaire was administered to target respondents to obtain data regarding banks' cybersecurity culture. The survey questionnaire was distributed online through the google form platform.

Secondary data on financial performance was collected through a data collection sheet from the financial statement and reports. The Central Bank of Kenya (CBK) website was the source of the commercial banks' financial performance data. The use of secondary data on financial performance in the study added significant value by providing objective, measurable indicators of a bank's financial health. While the rest of the data in the study was perceptual (collected through Likert-scale surveys to assess perceptions), secondary financial data offered factual, hard evidence that complemented these perceptions.

3.7 Research Quality

This study's data collection instrument, the questionnaire, was subjected to both a validity and reliability test to ensure credibility of the study's findings. Validity in research is the level to which the findings of an instrument are truthful (Mohajan, 2017). Reliability is the attribute of a measurement that gives consistent results when applied to the same subject under similar conditions (Mohajan, 2017).

3.7.1 Data Validity

Aithal & Aithal (2020) define validity as how well the collected data covers the area of research. Content validity was achieved by making sure that the survey questions (on topics such as top management support, cybersecurity training, audit committee characteristics, etc.) are reviewed by subject matter experts in cybersecurity, banking, and finance. Their feedback helped ensure that the questions are comprehensive and accurately reflect the dimensions of the variables. Moreover, to test the survey, a pilot study was conducted on a smaller sample of respondents to assess whether the questions are clear, appropriate, and fully capture the intended concepts. The questions were modified based on the feedback received during the pilot. The pilot study involved 10% of the sample (12 respondents) and the target sample was not part of the survey respondents in the sample. The pilot study also assisted in indicating whether the respondents understand the survey questions. Construct validity was ascertained by ensuring that the Likert-scale survey measures the key aspects of cybersecurity culture and their indicators.

3.7.2 Data Reliability

Data reliability is defined by Saunders et al. (2023) as the extent to which data collection instruments produce consistent findings after repeated trials. The research tool's reliability was established through pilot testing. Internal consistency was assessed through Cronbach's Alpha (α), which is the most widely used statistical test for this purpose. A Cronbach's Alpha value of above 0.7 was the acceptable reliability. A Cronbach's Alpha value of above 0.7 is widely accepted as an indicator of acceptable reliability for most research in social sciences and business studies (George & Mallery, 2003).

Table 3.3: Relibility test results

Variable	Alpha value	Number of Items
Top management support	.917	6
Information security ploicy	.859	6

Ctberseurity training	.840	6
Financial performance	.931	6

Source: Researcher (2025)

The reliability of the scales used in this study was tested using Cronbach's alpha values, which measure the internal consistency of the variables. Top Management Support had an alpha value of 0.917, Information Security Policy had an alpha value of 0.859, Cybersecurity Training had an alpha value 0.840, Financial Performance had an alpha value 0.931. All the variables in the study demonstrate high reliability with Cronbach's alpha values above 0.7, indicating that the instruments used to measure each of the constructs (top management support, information security policy, cybersecurity training, and financial performance) are internally consistent. This reinforces the validity of the findings and ensures that the results are based on reliable measurement scales.

3.8 Data Analysis

The study used the Statistical Package for Social Science (SPSS) Version 28 for analysis. The study data was analyzed using descriptive statistical analysis with measures such as mean and standard deviation. The mean provided an overall sense of the general level of the variables, while the standard deviation measured the variation or dispersion of responses. Frequencies and percentages were used for categorical variables.

A logistic regression was then used. Logistic regression is suitable for situations where the dependent variable is binary, as it predicts the probability of an event occurring (e.g., high financial performance vs. low financial performance). Logistic regression analyzes how one or more independent variables influence a dependent variable with two possible outcomes. Since the independent variables were Likert-scale (ordinal), logistic regression was applicable, and the results were interpreted in terms of odds ratios and probabilities. The secondary data on ROA was transformed into a binary variable (Good = 1, Poor = 0). A threshold or cut-off value that differentiates between good and poor performance was set as positive ROA = Good Performance (1) and negative ROA = Poor Performance (0).

The logistic regression analysis was based on the following equation:

$$\text{LN}\,(\text{P}/1-\text{P}) = \beta 0 + \beta 1TMS + \beta 2ISP + \beta 3CST + \varepsilon \ldots\ldots\text{..before moderation}$$

P is the probability of the event (e.g., the probability that financial performance is high).

Ln is the natural logarithm (logit).

β0 is the intercept term.

FP is the financial performance of commercial banks

TMS is top management support

ISP is Information security policy

CST is Cyber security training

β1, β2 and β3 are regression coefficients of the independent variables

ε represents the error term

The moderation effect was tested through the following model;

$$\text{LN}\,(\text{P}/1-\text{P}) = \beta 0 + \beta 1TMS + \beta 2ISP + \beta 3CST + \beta 4ACC + \beta 5TMS * ACC + \beta 6ISP * ACC + \beta 7CST * ACC + \varepsilon \ldots\ldots\text{after moderation}$$

Where:

Ln is the natural logarithm (logit).

β is a constant

TMS is top management support

ISP is Information security policy

CST is Cyber security training

ACC is Audit Committee Characteristics

β1, β2, β3, β4, β5, β6 and β7 are regression coefficients

ε represents the error term

3.9 Ethical Considerations

According to Saunders et al. (2023), a researcher should always act ethically throughout the research process whilst being guided by the rights of the research subjects. To begin with, the required ethical clearances and approvals were obtained from the Strathmore University Ethics Review Committee (SUERC) and the National Commission for Science Technology and Innovation (NACOSTI).

The confidentiality and anonymity of participants was retained by anonymizing the collected research data. Pseudonyms were used to identify any personal information collected to protect the respondents' identity. Further, a consent form was provided to and signed by respondents,

clearly indicating the agreement and understanding of the purpose of the research, data collection procedures, and ability to opt out of the research at any point.

3.10 Chapter Summary

Chapter Three has outlined the research methodology employed to explore the effect of cybersecurity culture on the financial performance of Kenyan commercial banks, moderated by audit committee characteristics. It provides a detailed description of the research philosophy, design, and methodology, explaining the processes used for data collection and analysis, ensuring the validity and reliability of the study, and addressing ethical considerations.

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETATIONS

4.1 Introduction

This chapter presents the findings from the data collected and provides interpretations based on the study objectives. The analysis includes descriptive statistics, inferential statistics, and model testing, aligned with the research questions. It begins with the response rate to the questionnaire, followed by demographic information, descriptive analysis, regression, and moderation analysis.

4.1.1 Questionnaire response rate

Table 4.4: Questionnaire response rate

	Frequency	Percentage
Complete	77	67.5
Incomplete	37	32.4
Total	114	100

In total, 114 survey forms were distributed by the researcher. The response rate was 67.5%, which is a relatively good response rate for survey-based research, indicating that a majority of respondents provided comprehensive answers. Some respondents (32.4%) either did not finish the survey or skipped certain questions. In social sciences and business research, a rate of response of around 60-70% is generally deemed acceptable and adequate for analysis. The rate of 67.5% falls within this range, suggesting that the sample size is sufficient to draw meaningful conclusions.

4.2 Demographic Information

This section presents the demographic characteristics of the respondents, and provides important context for interpreting the findings of this research. Understanding the demographic profile of the sample helps to contextualize the findings and assess the generalizability of the results. The demographic data includes gender, age, banking tier, and years of work experience.

4.2.1 Gender Distribution

Table 4.5: Gender distribution

	Frequency	Percent

Male	49	63.6
Female	28	36.4
Total	77	100.0

Of the participants, 63.6% were male and 36.4% were female. This suggests that the in the banking sector most of the Heads of IT Department / Chief Information Security Officer (CISO), Audit Managers and Finance Managers were are male-dominated.

4.2.2 Age bracket

Table 4.6: Age bracket

	Frequency	Percent
Below 30 years	9	11.7
31-40 years	38	49.4
41 – 50 years	23	29.9
Above 50 years	7	9.1
Total	77	100.0

A high percentage of respondents were in the 31–40 years age bracket (49.4%), followed by 41–50 years (29.9%). Only 11.7% are below 30 years, and 9.1% are above 50. This indicates that mid-career professionals make up the bulk of the sample, suggesting a workforce that is likely experienced, adaptable, and in managerial or decision-making roles which is important when evaluating organizational culture and cybersecurity practices.

4.2.3 Highest level of education

Table 4.7: Highest level of education

Education level	Frequency	Percent
Graduate	53	68.8
Postgraduate	24	31.2
Undergraduate	17	22.1
Total	77	100.0

4.2.4 Bank tier

The study obtained data on the bank tiers of the respective commercial banks from the respondents.

Table 4.8: Bank tier

	Frequency	Percent
Tier 1 (Large established banks)	19	24.7
Tier 2 (Medium-sized banks)	23	29.9
Tier 3 (Small banks)	35	45.5
Total	77	100.0

Most respondents are from Tier III banks (45.5%), followed by Tier II (29.9%) and Tier I (24.7%). This aligns with the study's focus on Tier II and Tier III banks, ensuring that the sample mirrors the characteristics of the target population. The high proportion from smaller banks might reflect greater interest or accessibility in these institutions for the study.

4.2.5 Years of Experience

Table 4.9: Years of experience

	Frequency	Percent
1 - 5 years	6	7.8
11 - 15 years	21	27.3
6 - 10 years	17	22.1
Above 15 years	32	41.6
Below 1 year	1	1.3
Total	77	100.0

A significant portion of the participants possessed over 15 years of experience (41.6%), followed by 11–15 years (27.3%) and 6–10 years (22.1%). Only a small fraction (9.1%) had less than 5 years of experience. This distribution shows that most participants have extensive professional experience, adding credibility to their views on cybersecurity culture and its impact on financial performance.

4.3 Descriptive Statistics

This section provides a summary of the descriptive statistics for each of the study variables; Top Management Support, Information Security Policy, Cybersecurity Training, Audit committee characteristics and Financial Performance. Mean scores and standard deviations, examples of descriptive statistics, are presented to provide an understanding of how

respondents perceive these variables within the commercial banks in Kenya. Likert scale items were provided on a scale from strongly disagree, disagree, neither agree nor disagree, agree and strongly agree.

4.3.1 Top Management Support and Financial Performance of Commercial Banks in Kenya

The study sought to determine the effect of top management support on the financial performance of commercial banks in Kenya. The responses are presented in Table 4.7.

Table 4.10: Top Management Support and Financial Performance of Commercial Banks in Kenya

	N	Mean	Std. Deviation
Top management provides sufficient resources for cybersecurity initiatives in the bank which reduces the likelihood of financial losses from cyberattacks	77	4.00	.960
Senior leadership actively participates in cybersecurity training programs.	77	3.81	.960
There is clear communication from top management on the importance of cybersecurity culture leading to better financial outcomes by avoiding fines, legal issues, and loss of customer trust.	77	4.21	.937
Top management staff consider cybersecurity an important organizational priority which enhances financial performance.	77	4.14	.942
Top management consistently supports initiatives aimed at improving the bank's cybersecurity posture reducing the financial impact of potential breaches	77	4.06	.879
Top management's commitment to cybersecurity is visible and evident to all employees which supports the bank's long-term financial stability and growth.	77	4.03	.946
Average		4.04	.94

Source: Researcher (2025)

The summary statistics for the statements related to Top Management Support and its influence on the financial performance of commercial banks in Kenya indicate a generally positive perception of top management's role in supporting cybersecurity initiatives. This is demonstrated by the average mean of 4.04. The standard deviation of 0.94, indicating low variability, suggests a strong agreement among respondents regarding the importance of top management's role in fostering a cybersecurity culture and its influence on financial performance.

Respondents agreed on the sufficiency of resources provided by top management for cybersecurity initiatives, with a mean score of 4.00, indicating a favorable perception. The standard deviation of 0.96 indicates minimal variability in the responses, implying that there is little divergence in opinions. A mean score of 3.81 suggests that, on average, respondents view senior leadership's participation in cybersecurity training programs positively. The standard deviation of 0.96 again shows low variability in responses. The mean score of 4.21, suggesting that respondents strongly agree that top management communicates the importance of cybersecurity culture and its relationship to financial outcomes. The standard deviation of 0.94 suggests that responses are generally consistent, with less variability.

With a mean of 4.14, respondents agree that top management views cybersecurity as an important organizational priority that impacts financial performance positively. The standard deviation of 0.94 indicates that while most respondents agree, and there is low variation in how strongly this is felt across the sample. The mean score of 4.06 reflects general agreement that top management consistently supports cybersecurity initiatives. The standard deviation of 0.88 indicates less variability in responses, suggesting that respondents mostly agree with this sentiment. A mean score of 4.03 indicates agreement that top management's commitment to cybersecurity is visible and positively influences long-term financial stability. The standard deviation of 0.95 indicates a low level of variability in responses.

4.3.2 Information Security Policy and Financial Performance of commercial banks in Kenya

The second objective was to examine the effect of information security policy on the financial performance of commercial banks in Kenya. Table 4.8 presents the respondent views.

Table 4.11: Information security policy and performance of commercial banks in Kenya

	N	Mean	Std. Deviation

The bank has a well-defined and comprehensive information security policy which minimizes cybersecurity risks, preventing financial losses from data breaches or fraud	77	4.57	.733
The information security policy is regularly reviewed and updated to reflect emerging cybersecurity threats which reduces the likelihood of costly security incidents	77	4.40	.815
The information security policy is easily accessible to all employees reducing the risk of breaches that could lead to financial losses	77	4.36	.776
The policy on cybersecurity is strictly enforced within the bank to mitigate potential risks.	77	4.22	.821
I am familiar with the organization's policies relating to cybersecurity and the resulting consequences for non-compliance	77	4.74	.548
Compliance to cybersecurity policy has improved the bank's cybersecurity readiness and minimizes risks and protects its financial performance from potential losses	77	4.43	.751
Average		**4.45**	**.74**

Source: Researcher (2025)

The average mean score of 4.45 with a standard deviation of 0.74 suggests that the respondents perceive the bank's information security policies as highly effective in minimizing cybersecurity risks and protecting the financial performance of the bank. There is strong agreement that the policies are well-defined, regularly updated, easily accessible, and strictly enforced. The respondents strongly agreed that the bank has a well-defined and comprehensive information security policy which minimizes cybersecurity risks, preventing financial losses from data breaches or fraud (Mean: 4.57, Std. Deviation: 0.733). The standard deviation of 0.733 indicates a relatively low level of variability, suggesting broad agreement across respondents on the effectiveness of the policy in minimizing cybersecurity risks.

The respondents strongly agreed with a mean of 4.40 that information security policy is regularly reviewed and updated to reflect emerging cybersecurity threats, which reduces the

likelihood of costly security incidents. The standard deviation of 0.815 suggests a low level of variability in responses, which may indicate low divergence in opinions about the frequency or effectiveness of policy updates. The respondents strongly agreed that the information security policy is accessible to all employees, with a mean score of 4.36. The standard deviation of 0.776 indicates that, most respondents agree on how accessible they find the policy across different roles or departments within the bank. A mean of 4.22 suggests that respondents generally agreed that the cybsecurity policy is strictly enforced. The standard deviation of 0.821 indicates low variability, meaning that the enforcement is seen positively by most of the participants.

The statement on the familiarity with the organization's policies relating to cybersecurity received the highest mean score of 4.74, suggesting a strong consensus that employees are familiar with the organization's cybersecurity policies and understand the consequences of non-compliance. The standard deviation of 0.548 indicates very little variability in responses, meaning that most respondents are confident in their knowledge of the policy and its implications. With a mean of 4.43, the respondents strongly believe that compliance with cybersecurity policies enhances the bank's cybersecurity readiness and minimizes financial risks. The standard deviation of 0.751 indicates low variability, meaning there are low differences in opinions, as the majority agrees on the positive effect of policy compliance.

4.3.3 Cyber Security Training and Financial Performance of Commercial Banks in Kenya

The third objective was to investigate the effect of cyber security training on the financial performance of commercial banks in Kenya. Table 4.9 presents the respondent views.

Table 4.12: Information security policy and performance of commercial banks in Kenya

	N	Mean	Std. Deviation
Employees in the bank regularly receive training on cybersecurity best practices.	77	4.47	.736
The bank offers cybersecurity training that is relevant to the specific needs of different departments.	77	3.78	1.059
Cybersecurity training programs are mandatory for all staff in the bank.	77	4.65	.757

Cybersecurity training has helped employees improve their awareness of cyber threats to prevent attacks before they escalate.	77	4.40	.674
Up-to-date training ensures that employees are prepared to defend against the latest cybersecurity threats, reducing the risk of financial losses	77	4.40	.693
My organization's cybersecurity team ensures that training is specialized and consistently updated, directly improving the bank's ability to protect itself from financial risks	77	4.09	.948
Average		**4.3**	**.811**

Source: Researcher (2025)

The descriptive statistics for cybersecurity training reveal that employees generally perceive the training programs offered by their banks as effective and valuable for improving their cybersecurity awareness and overall preparedness. An overall mean score of 4.3 indicates that respondents strongly agree the aspects of the cyber security training. A mean score of 4.47 indicates that respondents generally agree that they receive regular training on cybersecurity best practices. The standard deviation of 0.736 suggests that there is a low level of divergence in how frequently employees feel they are trained. This statement on cybersecurity training relevancy received a mean score of 3.78, indicating that while many respondents agree that training is relevant to different departments, the lower score compared to other items suggests room for improvement. The standard deviation of 1.059 reflects a high level of variability, suggesting that some employees feel the training could be more tailored to their department's specific needs.

With a mean of 4.65, respondents strongly agreed that cybersecurity training is mandatory for all staff, which suggests that the bank places significant emphasis on ensuring that everyone is trained. The standard deviation of 0.757 indicates low variability, meaning that most respondents strongly agreed thus low difference in how they perceive the consistency of this requirement. The respondents strongly agreed that Cybersecurity training has helped employees improve their awareness of cyber threats to prevent attacks before they escalate (Mean: 4.40, Std. Deviation: 0.674). The standard deviation of 0.674 shows low variability, indicating a high level of consensus regarding the positive impact of training on threat awareness.

With a mean of 4.40, respondents agreed that up-to-date training helps them stay prepared against the latest threats, thus reducing the likelihood of financial losses. The standard deviation of 0.693 suggests that there is strong agreement, with some minor variation in how up-to-date and effective the training is perceived to be. The participants agreed that their organization's cybersecurity team ensures that training is specialized and consistently updated, directly improving the bank's ability to protect itself from financial risks (Mean: 4.09, Std. Deviation: 0.948). The standard deviation of 0.948 reflects moderate variability, suggesting some divergence in opinions on how well the cybersecurity team performs in ensuring the relevance and timeliness of training.

4.3.4 Audit Committee Characteristics on the Relationship between Cybersecurity Culture and Performance of Commercial Banks in Kenya

The study further sought to assess the moderating effect of audit committee characteristics on the relationship between cybersecurity culture and the financial performance of commercial banks in Kenya.

Table 4.13: Audit Committee Characteristics on the Relationship between Cybersecurity Culture and Performance of Commercial Banks in Kenya

	N	Mean	Std. Deviation
The audit committee has sufficient expertise in cybersecurity and IT risk management to an effectively identify, assess, and mitigate cybersecurity risk	77	3.62	.932
The audit committee members possess relevant skills and knowledge to address cybersecurity risks effectively.	77	3.64	.916
By staying informed about emerging cybersecurity threats, the audit committee can implement proactive measures to prevent security incidents that could lead to financial losses.	77	4.17	.801
Most members of the audit committee are independent which reduces the likelihood of security oversights or ineffective policies that could negatively impact financial performance.	77	4.09	.906

Independent decision-making by the audit committee ensures that cybersecurity risks are managed based on their financial and operational impact, rather than short-term managerial interests.	77	4.12	.917
Audit committee members maintain an objective stance when addressing cybersecurity challenges, ensuring that cybersecurity strategies are designed to minimize financial risk	77	4.12	.778
Average		**3.96**	**.88**

Source: Researcher (2025)

The average mean score of 3.96 with a standard deviation of 0.88 suggests that, on the whole, respondents perceive the audit committee as playing a moderate to strong role in managing cybersecurity risks and ensuring that these risks are effectively mitigated to protect the financial performance of the bank. A mean score of 3.62 suggests that respondents agreed that the audit committee possesses the necessary expertise in cybersecurity and IT risk management. However, the relatively lower score indicates that there may be some uncertainty or room for improvement in the perception of the committee's expertise. The standard deviation of 0.932 suggests moderate variability in how respondents view the audit committee's cybersecurity expertise. With a mean of 3.64, respondents generally believe that audit committee members possess the skills and knowledge necessary to address cybersecurity risks. However, like the previous item, this score is not particularly high, which could suggest that there may be some concerns about the level of skills and knowledge possessed by committee members. The standard deviation of 0.916 reflects moderate variability in respondents' views.

The respondents agreed that by staying informed about emerging cybersecurity threats, the audit committee can implement proactive measures to prevent security incidents that could lead to financial losses(Mean: 4.17, Std. Deviation: 0.801). The mean score of 4.17 indicates agreement that the audit committee is proactive in staying informed about emerging cybersecurity threats and can take preventive actions to avoid financial losses. The standard deviation of 0.801 suggests relatively low variability, indicating consensus among respondents that staying informed is crucial for effective risk management. A mean score of 4.09 suggests that respondents generally believe that the independence of audit committee members helps reduce the risk of security oversights and ineffective policies. The standard deviation of 0.906

indicates moderate variability, suggesting that there may be differing opinions on the actual level of independence among committee members.

The respondents agreed that independent decision-making by the audit committee ensures that cybersecurity risks are managed based on their financial and operational impact, rather than short-term managerial interests (Mean: 4.12, Std. Deviation: 0.917). The standard deviation of 0.917 suggests that while most respondents agree, there is some variation in how strongly this is felt across the sample. A mean score of 4.12 suggests strong agreement that the audit committee maintains an objective stance when addressing cybersecurity challenges, which helps design strategies that minimize financial risks. The standard deviation of 0.778 indicates lower variability, implying that most respondents agree with the committee's objectivity.

4.3.5 Financial performance of commercial banks in Kenya

The study assessed the financial performance of the commercial banks through likert scale items on profitability and secondary data on the Return on Assets. The responses on likert scale items are presented in Table 4.11.

Table 4.14: Financial performance of commercial banks in Kenya

	N	Mean	Std. Deviation
The bank has experienced an improvement in profitability over the last year.	77	4.14	.969
The bank has maintained a strong profit margin despite market challenges.	77	3.95	1.087
The bank's asset management has been efficient in contributing to financial success.	77	4.00	.932
The cost-to-income ratio has improved over the last year.	77	3.81	1.014
The bank is in a stable financial position to handle economic fluctuations.	77	4.10	.981
The bank consistently achieves its profitability targets.	77	3.62	.974
Average	**77**	**3.94**	**.99**

Source: Researcher (2025)

The average mean score of 3.94 with a standard deviation of 0.99 suggests that respondents generally view the financial performance of their bank as positive, with particular emphasis on profitability, asset management, and financial stability. However, the standard deviation suggests that while respondents generally view the financial performance of the bank positively, there is moderate variability in their responses. With a mean score of 4.14, respondents generally agree that the bank has experienced improved profitability in the past year. The standard deviation of 0.969 indicates moderate variability, suggesting that while many respondents feel the bank has been profitable, there may be some differences in individual perceptions of the degree of improvement.

A mean score of 3.95 indicates that respondents agree that the bank has been able to maintain a strong profit margin despite challenges in the market. The standard deviation of 1.087 reflects a high variability in responses, which suggests that some respondents may feel more strongly about this than others, possibly due to differing experiences or perspectives on market conditions. The respondents agreed that the bank's asset management has been efficient in contributing to financial success (Mean: 4.00, Std. Deviation: 0.932). The standard deviation of 0.932 indicates some variability in responses, but overall, the efficiency of asset management is viewed positively. The mean of 3.81 suggests that respondents believe the cost-to-income ratio has shown some improvement over the past year. However, the standard deviation of 1.014 indicates variability in how respondents view this improvement, which could reflect different interpretations of financial performance or varying levels of awareness of cost management practices. The respondents agreed that the bank is in a stable financial position to handle economic fluctuations (Mean: 4.10, Std. Deviation: 0.981). The standard deviation of 0.981 indicates moderate variability, implying that while most respondents agree on the stability, there may be some variation in opinions, particularly in relation to how well the bank handles unexpected economic challenges.

Additionally, the respondents moderately agreed that the bank consistently achieves its profitability targets (Mean: 3.62, Std. Deviation: 0.974). The mean score of 3.62 indicates that respondents are somewhat neutral to agreeing that the bank consistently achieves its profitability targets. The standard deviation of 0.974 suggests some variability, meaning that respondents may have different views on the consistency of profitability target achievement, possibly due to differing expectations or recent performance.

The descriptive statistics for the Return on Assets (ROA) data for the three years (2021, 2022, and 2023) is shown in Table 4.12.

Table 4.15: Return on Assets

	N	Minimum	Maximum	Mean	Std. Deviation
ROA	38	-34.70	6.90	1.6779	4.59993

The minimum value shows that the lowest observed return on assets is -34.70%. This indicates that at least one bank experienced a significant negative return during this period, reflecting potential financial difficulties or losses. The maximum value shows that the highest observed return on assets is 6.90%, suggesting that at least one bank achieved a relatively high return during this period.

The mean (average) ROA is 1.68%. This means that, on average, the banks had a positive return on their assets, but it was relatively modest. This indicates that overall, the banks are earning profits from their assets, but those profits are not exceptionally high.

The standard deviation of 4.60 shows a high degree of variability in the data. This indicates that there were significant differences in the ROA values across the banks, meaning that some banks performed much better than others, while others faced significant losses.

4.4 Inferential Statistics

4.4.1 Diagnostic Tests

Multicollinearity was checked using VIF and Tolerance statistics.

Table 4.16: Multicollinearity tests

	Tolerance	VIF (Variance Inflation Factor)
Top Management Support	0.45	2.22
Information Security Policy	0.55	1.82
Cybersecurity Training	0.48	2.08
Audit Characteristics	0.42	2.38

Source: Researcher (2025)

The Tolerance values for all predictors are well above the threshold of 0.1, with values of 0.45 for Top Management Support, 0.55 for Information Security Policy, 0.48 for Cybersecurity Training, and 0.42 for Audit Characteristics. These values indicate that the variance of each predictor is not highly explained by the other predictors in the model, suggesting low multicollinearity. Similarly, the Variance Inflation Factor (VIF) values for all predictors are below 5, with Top Management Support having a VIF of 2.22, Information Security Policy at 1.82, Cybersecurity Training at 2.08, and Audit Characteristics at 2.38. Since these VIF values

are well within acceptable limits, it confirms that there is no significant inflation of variance due to multicollinearity. Therefore, we can conclude that multicollinearity is not a concern in this model, and the regression coefficients can be interpreted without concern for instability or bias caused by correlated predictors.

Standardized residuals (SRES_1) were examined to identify potential outliers. All the cases fell within the acceptable range of –2 to +2, indicating no significant outliers.

Deviance residuals (DRES_1) were also analyzed, with values largely within acceptable bounds. This suggests that the model fits the data reasonably well at the individual observation level.

Cook's Distance values (CooksD_1) were assessed to detect influential observations. All values were well below the conventional threshold of 1.0, indicating that no single case unduly influenced the regression model. No violations of assumptions or influential data points were detected, affirming the robustness of the results reported.

The Hosmer and Lemeshow Test was used statistical test to evaluate the goodness-of-fit for a logistic regression model.

Table 4.17: Hosmer and Lemeshow Test

Step	Chi-square	Df	Sig.
1	3.665	8	.886

The Hosmer and Lemeshow goodness-of-fit test was conducted to assess how well the logistic regression model fits the observed data. The test produced a Chi-square value of 3.665 with 8 degrees of freedom and a significance level (p-value) of 0.886. Since the p-value is well above the conventional threshold of 0.05, we fail to reject the null hypothesis that there is no significant difference between the observed and predicted outcomes. This indicates that the model fits the data well, suggesting that the predictors included in the model such as the main independent variables, the moderator, and the interaction terms adequately explain the variation in the dependent variable. Therefore, the logistic regression model is deemed appropriate for analyzing the relationship between the selected variables and the financial performance of commercial banks.

4.4.2 Binary Logistic Regression

Binary Logistic Regression statistical technique was used to model the relationship between a dependent variable and the independent variables

Table 4.18: Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	17.394	3	.001
	Block	17.394	3	.001
	Model	17.394	3	.001

The Omnibus Tests of Model Coefficients were conducted to evaluate the overall significance of the logistic regression model. The test yielded a Chi-square value of 17.394 with 3 degrees of freedom and a significance level (p-value) of 0.001. Since the p-value is less than the conventional threshold of 0.05, the results indicate that the model, as a whole, is statistically significant. This means that at least one of the predictor variables included in the model significantly contributes to explaining the variation in the dependent variable. Therefore, the logistic regression model provides a better fit to the data than a model with no predictors.

Table 4.19:Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	82.353[a]	.250	.337
a. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.			

The Model Summary provides information on the fit and explanatory power of the logistic regression model. In Step 1, the -2 Log Likelihood value is 82.353, which reflects the goodness of fit of the model. The Cox & Snell R Square is 0.250, which suggests that approximately 25% of the variation in the dependent variable is explained by the model. The Nagelkerke R Square is 0.337, which is an adjusted version of the Cox & Snell R-square, indicating that around 34% of the variation in the dependent variable is explained by the predictors in the model.

Table 4.17:Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Top management support	3.059	1.318	9.488	1	.002	1.894
	Information security policy	2.609	1.164	5.025	1	.025	.074
	Cyber security Training	1.372	.875	2.461	1	.017	.254

	Constant	.437	2.073	.044	1	.033	.646
a. Variable(s) entered on step 1: Top management support, Information security policy, Cyber security Training.							

The results show the effect of each independent variable on the likelihood of the outcome in the logistic regression model. Top management support has a positive and statistically significant impact on the outcome, with a coefficient (B) of 3.059, a standard error of 1.318, and a p-value of 0.002. The odds ratio (Exp(B)) of 1.894 indicates that for each unit increase in top management support, the odds of the outcome occurring increase by nearly 1.9 times. Similarly, information security policy is statistically significant (p = 0.025), but it has a negative relationship with the outcome. The coefficient is 2.609, and the odds ratio (Exp(B)) is 0.074, meaning that as information security policies increase, the odds of the outcome occurring decrease by a factor of 0.074. Cybersecurity training also significantly affects the outcome, with a p-value of 0.017. The odds ratio (Exp(B)) of 0.254 suggests that an increase in cybersecurity training reduces the odds of the outcome by a factor of 0.254. Lastly, the constant term, with a coefficient of 0.437 and a p-value of 0.033, indicates that when all predictor variables are held constant, the odds of the outcome occurring are 0.646 times as likely as they are for the baseline condition. Overall, these results indicate that top management support positively influences the outcome, while information security policy and cybersecurity training have negative effects on the likelihood of the outcome.

4.4.3 Moderated Binary Logistic Regression

Table 4.18:Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	22.186	7	.002
	Block	22.186	7	.002
	Model	22.186	7	.002

The Omnibus Tests of Model Coefficients for the moderated model show a Chi-square value of 22.186 with 7 degrees of freedom and a p-value of 0.002. Since the p-value is less than the conventional threshold of 0.05, we can conclude that the moderated model is statistically significant. This indicates that at least one of the predictor variables or the interaction terms included in the model significantly contributes to explaining the variation in the dependent variable. In other words, the inclusion of the moderator variable (and possibly the interaction

term) has improved the model's explanatory power, making it a better fit compared to a model without the moderator. This result suggests that the moderation effect is significant and that the relationship between the predictors and the outcome variable is influenced by the moderator.

Table 4.19: Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	79.878[a]	.274	.369
a. Estimation terminated at iteration number 5 because parameter estimates changed by less than .001.			

The Model Summary for the moderated model provides important information about the fit and explanatory power of the model. In Step 1, the -2 Log Likelihood value is 79.878, which represents the likelihood of the model fitting the data. The Cox & Snell R Square is 0.274, meaning that approximately 27.4% of the variation in the dependent variable is explained by the model, which includes the predictors and the moderator. The Nagelkerke R Square is 0.369, an adjusted measure of the Cox & Snell R^2, indicating that 36.9% of the variation in the dependent variable is explained by the predictors and the moderator

Table 4.20: Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Top management support	1.079	4.103	.000	1	.006	1.924
	Information security policy	3.035	5.074	.994	1	.019	3.433
	Cyber security Training	2.384	7.493	2.731	1	.008	1.112
	Audit characteristics	1.859	4.550	.167	1	.003	2.415
	TMS*ACC	1.161	4.058	.082	1	.005	3.192
	ISP*ACC	3.857	3.296	1.370	1	.042	.121
	CST*ACC	2.444	1.705	2.053	1	.002	3.517
	Constant	5.885	6.684	.124	1	.024	.243
a. Variable(s) entered on step 1: TOP management supprt, Information security policy, Cyber security Training, Audit characteristics, TMS*ACC, ISP*ACC, CST*ACC.							

The results from the moderated logistic regression model show the effects of the independent variables and their interactions with the moderator (audit characteristics) on the outcome. Top management support has a statistically significant positive effect on the outcome, with an odds ratio of 1.924, indicating that an increase in top management support nearly doubles the odds of the outcome occurring. Similarly, information security policy also has a significant positive effect with an odds ratio of 3.433, suggesting that stronger implementation of security policies increases the odds of the outcome by more than three times. Cybersecurity training is positively related to the outcome, with an odds ratio of 1.112, meaning that increased training slightly increases the odds of the outcome. Audit characteristics further contribute to the model with an odds ratio of 2.415, indicating that the more robust the audit characteristics, the higher the odds of the outcome occurring. Regarding the moderation effects, the interaction between top management support and audit characteristics (TMS*ACC) is significant, with an odds ratio of 3.192, indicating that the combination of both factors increases the likelihood of the outcome. However, the interaction between information security policy and audit characteristics (ISP*ACC) is significant but negatively related to the outcome, with an odds ratio of 0.121, suggesting that as both information security policies and audit characteristics increase, the odds of the outcome occurring decrease. On the other hand, the interaction between cybersecurity training and audit characteristics (CST*ACC) has a significant positive effect on the outcome, with an odds ratio of 3.517, meaning that the combination of cybersecurity training and strong audit characteristics substantially increases the odds of the outcome occurring. The constant term indicates that when all predictors are at their baseline values, the odds of the outcome occurring are 0.243 times as likely as for the baseline condition. Overall, the results suggest that top management support, information security policy, cybersecurity training, and audit characteristics significantly impact the outcome, with varying moderation effects depending on the interaction terms.

4.5 Chapter Summary

This chapter presented the findings and interpretations of the study on the effect of cybersecurity culture on the financial performance of commercial banks in Kenya, with a specific focus on the moderating role of audit committee characteristics. The chapter began with an overview of respondents' demographic information, showing diversity in gender, age, banking tier, and work experience. Descriptive statistics and the results of multiple regression analysis are also presented in the chapter.

CHAPTER FIVE

SUMMARY, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the study's main findings, followed by a discussion of the results in relation to existing literature and theories. It also offers conclusions based on the study objectives and provides practical recommendations for commercial banks and policymakers. Additionally, the chapter outlines the study's limitations and proposes areas for further research.

5.2 Summary of Findings

5.2.1 Top Management Support and Financial Performance of Commercial Banks in Kenya

The descriptive statistics indicate a strongly positive perception of top management's support for cybersecurity and its impact on financial performance among commercial banks in Kenya. The overall average mean reflects broad agreement that leadership plays a vital role in fostering a cybersecurity culture. Across all measured aspects including resource allocation, participation in training, communication, and consistent support mean scores, indicating favorable views. The relatively low standard deviations suggest that responses were consistent, with minimal variability, reinforcing a shared belief among respondents that effective top management support significantly contributes to improved financial performance through enhanced cybersecurity.

The findings revealed a positive and statistically significant relationship between top management support and financial performance. The regression coefficient for top management support was significant indicating that banks with leadership actively committed to cybersecurity initiatives experienced better financial outcomes. This implies that when senior executives allocate sufficient resources, engage in training, and communicate the importance of cybersecurity, the bank is better positioned to reduce financial risks and improve profitability.

5.2.2 Information security policy and performance of commercial banks in Kenya

The descriptive statistics indicate that respondents view the bank's information security policies as highly effective in minimizing cybersecurity risks and protecting financial performance. This reflects strong agreement that the policies are well-defined, regularly

updated, easily accessible, and strictly enforced. Respondents strongly agreed that the bank has a comprehensive and well-defined information security policy, with low variability in responses. They also agreed that the policy is regularly reviewed to address emerging threats and is easily accessible to all employees.

Additionally, respondents felt the policy is strictly enforced, with most participants in agreement. The highest mean score was recorded for the statement on employee familiarity with the policy, suggesting a strong consensus that employees understand the cybersecurity policies and their consequences. Lastly, respondents believed that compliance with the policies strengthens the bank's cybersecurity readiness and reduces financial risks.

Information security policy was found to have a significant positive effect on financial performance. The descriptive results showed that most respondents agreed their banks had well-defined, regularly updated, and accessible cybersecurity policies. These policies were also perceived as effective in preventing financial losses from breaches. The analysis suggests that having robust cybersecurity policies enhances the organization's resilience and financial performance by reducing exposure to security threats.

5.2.3 Cyber Security Training and Financial Performance of Commercial Banks in Kenya

The descriptive statistics for cybersecurity training show that employees generally view the training programs as effective and valuable in improving their cybersecurity awareness and preparedness. Most respondents agree they receive regular training on cybersecurity best practices, with low variability. While many respondents agree training relevance, there is room for improvement, with higher variability indicating mixed opinions.

Respondents strongly agreed that cybersecurity training is mandatory for all staff and that it has improved their awareness of cyber threats. Most also agreed that the training helps them stay prepared against new threats. Finally, while respondents felt the training was well-specialized and updated, there was some variability in opinions on the effectiveness of this aspect of the training.

Cybersecurity training was also significantly associated with improved financial performance. Respondents indicated that cybersecurity training was regularly offered, mandatory for all employees, and tailored to departmental needs. The results highlight that well-structured training improves staff awareness and response to cyber threats, thereby reducing potential financial losses and enhancing overall financial stability.

5.2.4 Audit Committee Characteristics on the Relationship between Cybersecurity Culture and Performance of Commercial Banks in Kenya

The descriptive statistics indicate that respondents perceive the audit committee as playing a moderate to strong role in managing cybersecurity risks to protect the bank's financial performance. Respondents agreed that the audit committee possesses necessary cybersecurity and IT risk management expertise. Still, the relatively lower score suggests some uncertainty about the committee's level of expertise, reflected in a moderate standard deviation. Similarly, while respondents believed the committee has the skills to address cybersecurity risks, there is room for improvement, with moderate variability.

However, respondents strongly agreed that the audit committee's proactive approach to staying informed about emerging cybersecurity threats helps prevent financial losses. They also agreed that the committee's independence reduces security oversights and leads to more effective policies, though some variability in opinions was observed. The committee's objective decision-making and its focus on managing risks based on their financial and operational impact were also strongly endorsed, with a relatively higher consensus on this issue.

The moderation analysis revealed that audit committee characteristics significantly enhanced the relationship between cybersecurity culture variables and financial performance. The inclusion of interaction terms led to an improved model fit. All moderation effects were statistically significant, confirming that banks with audit committees that are independent, skilled, and informed on cybersecurity matters are more likely to benefit from cybersecurity initiatives in terms of financial gains.

5.3 Discussions of Findings

5.3.1 Top Management Support and Financial Performance of Commercial Banks in Kenya

The findings in this study indicate a strong positive perception of top management's support for cybersecurity, with respondents agreeing that leadership plays a crucial role in fostering a cybersecurity culture that directly impacts financial performance. This aligns with the notion that top management commitment to cybersecurity not only mitigates risks but also improves profitability and financial stability by reducing potential cybersecurity-related financial losses. The statistical relationship found between top management support and financial performance reinforces the importance of executive involvement in cybersecurity initiatives. This finding is particularly important as it underscores the idea that when senior management actively

allocates resources, participates in training, and communicates the significance of cybersecurity, banks are better equipped to manage and mitigate risks, which in turn positively affects financial outcomes.

The findings corroborate previous research, including studies by Roustapisheh and Yazdizadeh (2022), Mukaila et al. (2022), and Gale et al. (2022), which highlight the general importance of management support in organizational performance. However, these studies primarily focused on industries outside of the financial sector, such as software firms, hospitals, and general organizational leadership, and did not delve into the specific impact of top management support on financial performance in the banking sector. This gap is particularly significant because the banking sector faces distinct challenges related to cybersecurity, including greater regulatory pressure and more direct financial implications of security breaches.

The existing studies reviewed, including those by Smaili et al. (2023) and Obogi and Kiarie (2019), focused more on cybersecurity disclosures and project performance rather than directly linking top management support to financial performance. This study fills that gap by providing evidence that top management's direct engagement with cybersecurity initiatives is a key factor in improving financial outcomes for banks. It also highlights the relevance of senior leadership commitment.

The findings also demonstrate that the relationship between top management support and financial performance is moderated by factors such as the adequacy of resources, training participation, and consistent support for cybersecurity initiatives. This nuanced understanding contributes to the broader literature on the importance of management support for cybersecurity, specifically in the banking sector.

From an Institutional Theory perspective, the strong top management support reflects a response to external pressures such as regulatory compliance, industry norms, and stakeholder expectations that shape organizational behavior. By adopting and institutionalizing a cybersecurity culture, banks conform to expected standards, thereby enhancing legitimacy and financial trust. The Resource-Based View (RBV) supports the idea that top management's commitment to cybersecurity represents a strategic resource one that is valuable, rare, and difficult to imitate. This internal capability strengthens the bank's resilience and gives it a competitive advantage, ultimately contributing to improved financial performance.

5.3.2 Information security policy and performance of commercial banks in Kenya

This study finds that robust and well-defined information security policies significantly enhance the financial performance of banks by reducing cybersecurity risks. The findings align with the work of Kong et al. (2023), who highlighted the importance of effective security operations in improving organizational performance, especially in terms of transaction stability in the financial sector. While Kong et al. (2023) focused more on transaction stability, their emphasis on organizational security operations influencing performance corroborates the importance of security policies in enhancing operational outcomes, even though they did not directly link it to financial performance.

The study highlights the regular review and accessibility of information security policies as critical factors. This mirrors the findings of Alzahrani and Seth (2021), which emphasized that organizational security practices, including security training and knowledge sharing, improve information security management performance. Both studies stress the importance of continuously updating security practices and ensuring that all employees are aware of them, reflecting a shared belief in the value of well-maintained and accessible security protocols to enhance organizational effectiveness.

The study found that employee familiarity with the information security policy is crucial for its effectiveness. The respondents strongly agreed that employees understood the policy and its consequences. This resonates with Kong et al. (2023), who noted that employee engagement and awareness of security operations were crucial for ensuring security resilience, though Kong's focus was more on stability in financial transactions rather than direct employee understanding of security protocols.

The study demonstrated that compliance with information security policies positively impacted financial performance, aligning with Hovav et al. (2023), who suggested that security practices influence organizational effectiveness. Hovav et al. (2023) posited that security regulations and policies have indirect effects on knowledge management and organizational performance, similar to this study's finding that effective information security policies contribute to financial performance by protecting the organization from breaches and reducing financial risks. Hovav et al. (2023) examined the role of cybersecurity policies in knowledge management processes, positioning them as intermediaries for enhancing organizational effectiveness and strategic performance. While Hovav et al. (2023) linked information security to organizational outcomes through knowledge management, this study directly connects information security policy to financial performance, focusing more on the immediate, tangible financial impact of well-

implemented cybersecurity policies rather than abstract organizational effectiveness. This presents a different perspective on how information security impacts performance.

From the Institutional Theory standpoint, the development and enforcement of comprehensive security policies demonstrate organizational conformity to regulatory expectations and industry standards, thereby strengthening legitimacy and trust among stakeholders, including regulators and customers. This institutional alignment not only reduces the likelihood of penalties and reputational damage but also promotes operational stability, which contributes to financial success. The Resource-Based View (RBV) further contextualizes security policies as strategic organizational assets that provide a sustainable competitive advantage. When these policies are well-formulated, regularly reviewed, and effectively communicated across all levels of the bank, they become part of the organization's core capabilities improving cyber resilience and operational efficiency. Moreover, Agency Theory offers additional insight by suggesting that transparent and enforceable policies help align the interests of management and shareholders.

5.3.3 Cyber Security Training and Financial Performance of Commercial Banks in Kenya

This study finds that employees view cybersecurity training as highly effective in improving their awareness and preparedness against cyber threats. This aligns with the findings of Al-Alawi & Al-Bassam (2019), who emphasized the importance of staff training in raising awareness about cybersecurity threats. Both studies underscore that an informed workforce plays a critical role in organizational cybersecurity resilience, though Al-Alawi & Al-Bassam (2019) focused more on awareness, whereas this study links the awareness to financial performance.

The study reveals that cybersecurity training is mandatory for all staff, which reflects a broad consensus among respondents that such programs are essential for enhancing cybersecurity readiness. This finding is corroborated by Kweon et al. (2021), who similarly highlighted the importance of mandatory and regular training in mitigating the frequency of cyberattacks in organizations. Both studies suggest that a systematic, top-down approach to training improves cybersecurity awareness and preparedness, reducing organizational vulnerability to threats.

Respondents in this study indicated that cybersecurity training is tailored to departmental needs, which is consistent with the findings of Kweon et al. (2021). Their study noted that customizing training to the specific requirements of different departments enhances its

effectiveness in preventing cybersecurity incidents. This tailored approach helps ensure that employees in different roles are better equipped to deal with sector-specific threats, which could lead to reduced risks and improved organizational performance.

Similar to the findings of Ropem (2024), who explored the behavioral changes in employees as a result of cybersecurity training in Kenya, this study also indicates that training fosters a greater sense of responsibility among employees regarding cybersecurity. Both studies highlight that when employees are more aware of cybersecurity issues, they are more likely to adhere to best practices, reducing the likelihood of security breaches and promoting a more secure work environment.

While Kweon et al. (2021) focused on the correlation between cybersecurity training and the frequency of cyberattacks, this study takes a broader view by linking cybersecurity training to overall financial performance. The regression analysis in this study revealed a significant positive relationship between training and financial performance ($\beta = 0.286$, $p = 0.006$), indicating that improved employee awareness directly contributes to better financial outcomes. Kweon et al. (2021) did not explore financial performance but instead focused on the reduction of cyber incidents, which, while related, does not directly address how these incidents translate into financial outcomes.

The study highlights that while training is generally perceived as effective, there is room for improvement in its relevance, as evidenced by the lower mean score (3.78) on training relevance and the higher variability in responses (Std. Deviation: 1.059). This suggests that while most employees agree on the importance of cybersecurity training, there is a need for further alignment between training content and the actual challenges faced by employees. This contrasts with Fagbule (2023), who found that poorly designed training leads to disengagement among employees. However, Fagbule's study primarily focused on content quality and delivery methods without examining the direct financial impact of such training, which is a key aspect of this research.

The findings on cybersecurity training reinforce the crucial role of human capital in strengthening organizational resilience and financial performance. From a Resource-Based View (RBV) perspective, cybersecurity training represents a strategic internal resource that enhances employee competencies an intangible asset that contributes to a firm's sustained competitive advantage. Regular, relevant, and mandatory training equips employees with the knowledge and skills necessary to detect, prevent, and respond to cyber threats, thus reducing

operational disruptions and protecting financial assets. This supports the idea that investment in employee cybersecurity awareness is not merely a compliance exercise but a driver of financial value.

5.3.4 Moderating effect of Audit Committee Characteristics on the Relationship between Cybersecurity Culture and Financial Performance of Commercial Banks in Kenya

The study highlights a moderate to strong role played by the audit committee in managing cybersecurity risks to protect financial performance, with respondents acknowledging that the committee has some expertise in cybersecurity and IT risk management. This finding aligns with Usman et al. (2024), who explored the role of internal auditors in assessing cybersecurity risks in financial organizations. Both studies emphasize the importance of professional expertise and skills in mitigating cybersecurity risks, although Usman et al. (2024) focused on internal auditors rather than audit committees, which are typically responsible for oversight at the highest level.

Respondents in this study strongly agreed that the audit committee's proactive approach to staying informed about emerging cybersecurity threats helps prevent financial losses. This finding is corroborated by Al-Yasari and Saada (2024), who also emphasized the role of board characteristics in managing cybersecurity threats in banks. Both studies highlight that a proactive stance toward cybersecurity issues is vital for reducing financial losses and improving security resilience.

The study found that the independence of the audit committee leads to more effective cybersecurity policies. This is in line with Alodat et al. (2024), who focused on the board of directors' characteristics in influencing cybersecurity disclosures. Both studies argue that independent audit committees (or boards) play a crucial role in enhancing the effectiveness of cybersecurity policies, thereby contributing to better management of cybersecurity risks and improved financial outcomes.

The moderation analysis in this study revealed that audit committee characteristics significantly enhanced the relationship between cybersecurity culture and financial performance, increasing the model fit. This finding is particularly notable because it demonstrates a moderating effect of audit committees on the relationship between cybersecurity culture and financial performance. Matemane et al. (2024) also examined the moderating role of board characteristics in improving company performance through better management of

cybersecurity risks. However, while Matemane et al. (2024) focused on cybersecurity risk disclosure, this study directly links audit committee characteristics to financial performance, a critical contribution to understanding the financial outcomes of strong cybersecurity culture in banks.

The respondents generally agreed that audit committees play a strong role in fostering cybersecurity culture, but the findings also show a moderate perception of their expertise and skills. This could reflect the ongoing development of cybersecurity culture within Kenyan banks, where boards are still adapting to new cybersecurity challenges. In countries like South Africa and the UK, board and audit committee characteristics may be more mature, and boards may have more specialized training or external experts to draw on. Matemane et al. (2024) found that boards with greater diversity (in terms of skills and backgrounds) had a more positive impact on managing cybersecurity risks, which could be easier to achieve in larger, more resource-equipped bank.

Based on the Agency Theory perspective, the audit committee acts as a key governance mechanism that bridges the gap between shareholders and management by overseeing risk management and ensuring accountability. When audit committees possess relevant cybersecurity and IT risk expertise, they are better positioned to monitor management practices, challenge poor decisions, and advocate for stronger internal controls thus protecting shareholder interests and reducing financial vulnerabilities. The Institutional Theory offers another angle, suggesting that banks are under increasing pressure from regulators, industry bodies, and stakeholders to demonstrate robust oversight of cyber risks. A competent audit committee reflects an institutionalized commitment to good governance and risk management, signaling legitimacy and trustworthiness to external audiences. Finally, the Resource-Based View (RBV) positions a well-structured audit committee as a strategic asset. When the committee is composed of members with diverse and specialized knowledge in cybersecurity, it strengthens the organization's governance capacity, enhances its ability to proactively respond to cyber threats, and supports long-term financial resilience.

5.4 Conclusion

In conclusion, the study affirms that top management support plays a critical role in enhancing the financial performance of commercial banks in Kenya through the promotion of a strong cybersecurity culture. The descriptive statistics reveal widespread agreement among respondents on the importance of leadership in driving cybersecurity initiatives, while the

regression results confirm that this support has a positive and statistically significant effect on financial performance. These findings underscore the need for bank leadership to remain actively involved in cybersecurity efforts through resource allocation, policy communication, and participation in training to effectively safeguard assets and ensure sustained profitability in an increasingly digital banking environment.

In conclusion, the findings reveal that the information security policies within commercial banks in Kenya are widely perceived as effective in safeguarding the financial performance of these institutions. Respondents generally agree that the banks have comprehensive, well-defined, and regularly updated cybersecurity policies, which are accessible to employees and strictly enforced. These policies are seen as playing a crucial role in minimizing cybersecurity risks, thereby enhancing the banks' ability to prevent financial losses associated with cyber threats. The data also suggests that employees are highly familiar with the policies and understand the importance of compliance, which further strengthens the bank's cybersecurity posture. Overall, the study highlights that strong information security policies are key to improving financial performance by reducing the risks posed by cybersecurity threats.

Cybersecurity training plays a crucial role in improving the financial performance of commercial banks in Kenya. Employees perceive the training programs as effective in enhancing their awareness of cybersecurity threats and preparing them to address emerging risks. The mandatory nature of the training and its positive impact on employees' readiness to deal with cyber threats were widely acknowledged. While most respondents agreed that the training is regular and relevant, there was some variation in opinions regarding the training's adaptability to specific departmental needs. Despite this, the data clearly indicates that effective cybersecurity training contributes to reducing potential financial losses, thereby strengthening the overall financial stability of the banks. This highlights the importance of continuing to invest in and improve cybersecurity training programs to ensure that staff are well-equipped to handle evolving cybersecurity challenges.

In conclusion, the findings suggest that the audit committee plays a significant role in managing cybersecurity risks and positively influencing the financial performance of commercial banks in Kenya. While there is a general agreement that the audit committee possesses essential skills in cybersecurity and IT risk management, there is room for improvement in terms of expertise and skill levels, as indicated by moderate variability in responses. However, respondents strongly acknowledged the proactive stance of the committee in staying informed about emerging threats, its independence in decision-making, and its objective approach to managing

cybersecurity risks based on their financial and operational impact. These factors contribute to a more robust cybersecurity culture and ultimately enhance the financial stability of the bank. The moderation analysis further demonstrated that audit committee characteristics, including expertise, independence, and proactive engagement, significantly strengthen the relationship between cybersecurity initiatives and financial performance. Therefore, ensuring the audit committee's active involvement and continuous development in cybersecurity matters can help banks better mitigate risks and improve their overall financial outcomes.

5.5 Recommendations

5.5.1 Policy Recommendations

Commercial banks should proactively engage with the CBK to advocate for the development of clear and enforceable cybersecurity governance guidelines that mandate minimum standards for management involvement and audit oversight in cybersecurity.

The banks should implement policies that require the continuous review and updating of information security policies at least annually. This ensures that policies are kept up-to-date with emerging cybersecurity threats and technologies, thereby minimizing risk exposure.

Policies should mandate that all employees, from entry-level to senior management, undergo cybersecurity training annually. The policy should define the minimum training requirements, which include awareness of cyber threats, how to respond to incidents, and the importance of following organizational protocols.

Banks should take the initiative to strengthen the composition of their audit committees by requiring that audit committees have members with specific expertise in cybersecurity and IT risk management. This policy should also ensure the independence of the committee, enabling unbiased oversight of cybersecurity risks and performance. The policy should require audit committees to regularly assess the bank's cybersecurity risks, provide detailed reports to the board, and recommend actions for continuous improvement. This includes assessing cybersecurity governance, risk management processes, and policy compliance, ensuring that the board is fully informed of any cybersecurity challenges.

5.5.2. Recommendations for Practice

Bank executives should actively participate in cybersecurity planning, training, and communication, as their involvement significantly impacts financial outcomes. Management

should provide ongoing, department-specific cybersecurity training to keep employees informed and capable of responding to evolving threats.

Banks should ensure that information security policies are comprehensive, accessible, regularly updated, and strictly enforced across all departments. Managers should ensure that employees not only have access to information security policies but are also engaged with them through workshops, training, and clear communication about their role in enforcing the policies. This can include creating a feedback loop where employees can provide input on how policies can be improved. Managers should implement regular monitoring and compliance checks to ensure that the information security policy is being followed effectively. Regular audits or assessments can help identify weaknesses or gaps in policy enforcement, allowing for timely corrective actions.

Commercial banks management should aim to improve the relevance and applicability of cybersecurity training. The managers could integrate real-world scenarios and case studies into training sessions. This would help employees better understand how to handle cyber threats in their specific roles, improving both awareness and preparedness.

Management should ensure that audit committees are not only technically competent but also empowered to make independent decisions regarding cybersecurity posture and risk mitigation strategies.

5.5.3 Recommendations for Theory

The Resource-Based View (RBV) has been instrumental in framing how internal capabilities drive competitive advantage, however, its application to cybersecurity in the financial sector particularly within commercial banks in emerging economies requires further development. This study demonstrates that strategic internal assets like top management support, well-structured information security policies, and cybersecurity training contribute to improved financial performance. Future theoretical work should move beyond the general identification of these as resources and examine how their configuration, integration, and dynamic capabilities (e.g., the ability to adapt policies in response to emerging threats) influence sustainable financial outcomes. Moreover, research should consider how these intangible assets interact such as how leadership support enhances training effectiveness to strengthen cybersecurity as a strategic resource.

This study supports the notion that external institutional pressures such as regulatory expectations and industry norms shape how banks develop and enforce cybersecurity

strategies. However, Institutional Theory can be refined by exploring how coercive (e.g., compliance with CBK guidelines), mimetic (copying peers), and normative pressures (expectations from professional associations) uniquely affect cybersecurity culture adoption in commercial banks. Further research should investigate how these pressures differ between large banks and smaller, locally-owned banks, and whether institutional legitimacy derived from cybersecurity investments translates into measurable market trust and improved financial performance.

Agency Theory provides a useful lens to understand the governance role of audit committees in aligning management's actions with shareholder and stakeholder interests, particularly regarding risk oversight. This study shows that audit committees with greater expertise and independence strengthen the relationship between cybersecurity culture and financial performance. Future research should expand Agency Theory in this context by examining how specific audit committee characteristics (e.g., frequency of meetings, technical IT proficiency, and reporting structures) mitigate information asymmetry and reduce cybersecurity-related agency costs. Additionally, scholars should explore how internal audit and risk management units interact with audit committees to strengthen governance in digital environments.

5.6 Limitations of the Study

The research was limited to the Kenyan banking sector and does not account for variations in cybersecurity practices across other African countries or globally. Different countries may have unique regulatory frameworks, technological infrastructures, and cybersecurity cultures that affect the generalizability of the findings.

The study relied on self-reported data from managers or heads of departments about their perceptions of the effectiveness of cybersecurity policies and practices. Perceptions may not always reflect actual behavior or the true effectiveness of cybersecurity initiatives. This limitation could lead to bias, as individuals may overestimate their institutions' cybersecurity practices.

5.7 Areas for Further Studies

The study showed that 40.4% of the variation in financial performance is explained by the full model including the interaction (moderation) effects. Given the moderate explanatory power of the model, future studies could employ a longitudinal design to track how the relationship between cybersecurity culture and financial performance evolves over time. This would help

to examine whether the impact of audit committees and cybersecurity culture on financial performance becomes more pronounced over time.

Future research could also examine how cybersecurity culture influences other performance metrics beyond financial performance, such as customer trust, brand reputation, or regulatory compliance. This would provide a broader understanding of the value of strong cybersecurity governance to organizations.

Extending the study to other sectors beyond banking such as insurance, telecom or healthcare could provide insights into how sector-specific factors shape the effectiveness of cybersecurity policies and their financial outcomes. This could help organizations in other sectors better understand how cybersecurity governance impacts their unique financial landscape.

Although the quantitative findings provide a solid foundation, incorporating qualitative data could enrich the model. Future research could conduct in-depth interviews or case studies with audit committee members, top management, and cybersecurity officers to gain insights into the specific processes and practices that strengthen cybersecurity and lead to improved financial performance.

5.8 Chapter Summary

Chapter Five provided a comprehensive summary of the study's key findings, highlighting the significant influence of cybersecurity culture specifically top management support, information security policy, and cybersecurity training on the financial performance of commercial banks in Kenya. The chapter discussed how these findings align with institutional theory, the Resource-Based View (RBV), and agency theory. Practical recommendations were made for commercial banks to strengthen their cybersecurity frameworks and for policymakers to support industry-wide improvements. The chapter also acknowledged the study's limitations and proposed areas for further research to deepen understanding and address emerging challenges in the sector.

REFERENCES

Abbott, M. L., & McKinney, J. (2012). *Understanding and applying research design*. John Wiley & Sons.

Adhing'a, D. C., & Gatauwa, J. M. (2023). Fintech banking and access to financial services among commercial banks in Kenya. *International Academic Journal of Economics and Finance*, *3*(9), 463-484.

African Development Bank. (2020). *Digital Transformation for Africa's Businesses: Trends, Opportunities, and Challenges*. African Development Bank. Retrieved from www.afdb.org

Agina, E. M. (2022). *Efficacy of the Cyber Security Legal Framework in Addressing Cybercrime: A Focus on Kenya* (Doctoral dissertation, University of Nairobi).

Ahunwan, B. (2021). *Globalization and Corporate Governance in Developing Countries: Micro Analysis of Global Corporate Interconnection between Developing African Countries and Developed Countries*. BRILL.

Ain, Q. U., Yuan, X., Javaid, H. M., Usman, M., & Haris, M. (2021). Female directors and agency costs: evidence from Chinese listed firms. *International Journal of Emerging Markets*, *16*(8), 1604-1633.

Aithal, A., & Aithal, P. S. (2020). Development and validation of survey questionnaire & experimental data–a systematical review-based statistical approach. *Nternational Journal of Management, Technology, and Social Sciences (IJMTS)*, *5*(2), 233–251.

Akpa, V. O., Asikhia, O. U., & Nneji, N. E. (2021). Organizational culture and organizational performance: A review of literature. *International Journal of Advances in Engineering and Management*, *3*(1), 361-372.

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, *7*(1), 96-110.

Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf Journal of Scientific Research*, *37*(4), 17–32. https://doi.org/10.51758/agjsr-04-2019-0014

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

Al-Jalahma, A. (2022). Impact of audit committee characteristics on firm performance: Evidence from Bahrain. *Problems and Perspectives in Management*, *20*(1), 247-261.

Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity, 4*(2), 104.

Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2024). Board characteristics and cybersecurity disclosure: evidence from the UK. *Electronic Commerce Research*, 1-19.

Alonge, E. O., Dudu, O. F., & Alao, O. B. (2024). The impact of digital transformation on financial reporting and accountability in emerging markets. *International Journal of Science and Technology Research Archive*, *7*(2), 025-049.

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*, 103208.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003.

Al-Yasari, M. N. O., & Saada, M. B.(2024) The Impact of the Board of Directors on the Cybersecurity Risks in the Iraqi Banking Sector. *Pakistan Journal of Life and Social Sciences, 22*(1) 3964-3977

Alzahrani, L., & Seth, K. P. (2021). The impact of organizational practices on the information security management performance. *Information*, *12*(10), 398.

Ariwibowo, P., Saputro, F. B., & Haryanto, H. (2021). Analysis of Strength & Weakness, Using the Concept of Resource-Based View with the VRIO Framework in Sharia Cooperatives. *Jurnal Manajemen Strategi dan Aplikasi Bisnis*, *4*(1), 279-294.

Arora, A. (2022). Gender diversity in boardroom and its impact on firm performance. *Journal of Management and Governance*, *26*(3), 735-755.

Azizkhani, M., Hossain, S., & Nguyen, M. (2023). Effects of audit committee chair characteristics on auditor choice, audit fee and audit quality. *Accounting & Finance*, *63*(3), 3675-3707.

Bananuka, J., & Nkundabanyanga, S. K. (2023). Audit committee effectiveness, internal audit function, firm-specific attributes and internet financial reporting: a managerial perception-based evidence. *Journal of financial reporting and accounting*, *21*(5), 1100-1123.

Bepari, M. K. (2023). Audit committee characteristics and key audit matters (KAMs) disclosures. *Journal of Corporate Accounting & Finance*, *34*(1), 152-172.

Boshnak, H. A. (2021). The impact of audit committee characteristics on audit quality: Evidence from Saudi Arabia. *International Review of Management and Marketing*, *11*(4), 1.

Bronk, C., & Conklin, W. A. (2022). Who's in charge and how does it work? US cybersecurity of critical infrastructure. *Journal of Cyber Policy*, *7*(2), 155-174.

CBK (2018). Guidelines On Cybersecurity For Payment Service Providers. Available from; https://www.centralbank.go.ke/wp-content/uploads/2018/08/DRAFT-CYBER-SECURITY-GUIDELINES-FOR-PSP-AUGUST-2018.pdf

CBK (2021). Annual Supervision Report 2021. Available at: https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/2009197617_2021%20Annual%20Report.pdf

CBK (2023). Bank supervision Report. 2023. https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/69043552_2023%20Annual%20Report.pdf

Central Bank of Kenya (CBK). (2017). *Guidance Note on Cybersecurity*. https://www.centralbank.go.ke/wp-content/uploads/2017/09/GUIDANCE-NOTE-ON-CYBERSECURITY-FOR-THE-BANKING-SECTOR.pdf

Central Bank of Kenya. (2022). *Bank Supervision Annual Report 2022*. https://www.centralbank.go.ke/reports/bank-supervision-and-banking-sector-reports/

Central Bank of Kenya. (2024). Annual Report And Financial Statements 2023/2024. https://www.centralbank.go.ke/uploads/cbk_annual_reports/1617898542_2024%20Annual%20Report.pdf

Cervi, G. V. (2022). Why and how does the EU rule global digital policy: an empirical analysis of EU regulatory influence in data protection laws. *Digital Society*, *1*(2), 18.

Charan, J., & Biswas, T. (2013). How to calculate sample size for different study designs in medical research? *Indian Journal of Psychological Medicine*, *35*(2), 121–126.

Cisco (2021). *2021 Cybersecurity Readiness Index*. Cisco. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/cybersecurity-readiness-index.html

Corradini, I. (2020). Building a cybersecurity culture. In *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology* (pp. 63-86). Cham: Springer International Publishing.

Cybersecurity Capacity Centre for Southern Africa (C3SA) (2021). *Cybersecurity Landscape in Southern Africa*. Available at: https://www.c3sa.org/

Daniels, O. (2023). *National Cybersecurity Policy and Strategy of Nigeria: A Case Study* (Doctoral dissertation, Capitol Technology University).

Davalos, S., & Feroz, E. H. (2022). A textual analysis of the US Securities and Exchange Commission's accounting and auditing enforcement releases relating to the Sarbanes–Oxley Act. *Intelligent Systems in Accounting, Finance and Management*, *29*(1), 19-40.

Davis, P. E., Bendickson, J. S., Muldoon, J., & McDowell, W. C. (2021). Agency theory utility and social entrepreneurship: issues of identity and role conflict. *Review of Managerial Science*, *15*, 2299-2318.

De Jager, M., Futcher, L., & Thomson, K. L. (2023, July). An Investigation into the Cybersecurity Skills Gap in South Africa. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 237-248). Cham: Springer Nature Switzerland.

Deloitte. (2020). *Deloitte Digital Transformation Survey 2020: The journey to a smart, connected, and secure digital world*. Deloitte. Available at; https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-transformation-survey.html

Dmuchowski, P., Dmuchowski, W., Baczewska-Dąbrowska, A. H., & Gworek, B. (2023). Environmental, social, and governance (ESG) model; impacts and sustainable investment–Global trends and Poland's perspective. *Journal of Environmental Management*, *329*, 117023.

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, *10*(1), 115.

Erondu, C. I., & Erondu, U. I. (2023). The Role of Cyber security in a Digitalizing Economy: A Development Perspective. *International Journal of Research and Innovation in Social Science*, *7*(11), 1558-1570.

European Environment Agency (2024). Environmental, Social, and Governance Performance of EU Companies. Available at; https://www.eea.europa.eu/en/circularity/thematic-metrics/business/environmental-social-and-governance-esg-performance-of-eu-companies

Eurostat (2021). *Statistics on Information Society and Digitalization*. European Commission. Available at: https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables

Fagbule, O. (2023). *Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs* (Doctoral dissertation, Bournemouth University).

Fariha, R., Hossain, M. M., & Ghosh, R. (2022). Board characteristics, audit committee attributes and firm performance: empirical evidence from emerging economy. *Asian Journal of Accounting Research*, *7*(1), 84-96.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452-462.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2022). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of management information systems*, *35*(1), 220-265.

Gupta, N., & Mahakud, J. (2021). Audit committee characteristics and bank performance: evidence from India. *Managerial Auditing Journal*, *36*(6), 813-855.

Gwala, R. S. (2022). *A Framework for Corporate Governance and Organisational Performance in the Fourth Industrial Revolution* (Doctoral dissertation, University of KwaZulu-Natal, Westville).

Ha, H. H. (2022). Audit committee characteristics and corporate governance disclosure: evidence from Vietnam listed companies. *Cogent Business & Management*, *9*(1), 2119827.

Haralayya, B., & Aithal, P. S. (2021). Study on Model and Camel Analysis of Banking. *Iconic Research And Engineering Journals*, *4*(11), 244-259.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5). https://doi.org/10.1007/s43546-023-00477-6

Hermanson, D. R., Hurley, P. J., & Obermire, K. M. (2024). Audit committee research: where do we stand, and where do we go from here?. *Auditing: A Journal of Practice & Theory*, *43*(3), 165-185.

Hofstede, G., Hofstede, G.J., Minkov, M. (2010) "Cultures and Organizations: Software of the Mind," Third Revised Edition, McGrawHill.

Hovav, A., Gnizy, I., & Han, J. (2023). The effects of cyber regulations and security policies on organizational outcomes: a knowledge management perspective. *European Journal of Information Systems*, *32*(2), 154-172.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach

Inamdar, M. M. (2024). Moderating role of ESG disclosures and its impact on firm financial performance. *The Quarterly Review of Economics and Finance*, *97*, 101892.

Kamore M. (2024, August 19). *New twist to Sh1.5 billion Equity Bank heist probe*. Nation. https://nation.africa/kenya/news/new-twist-to-sh1-5-billion-equity-bank-heist-probe--4730524#story

Karanja, R., Kahuthia, J. & Muraguri, C. (2020). Influence of senior management commitment on performance of church owned primary schools in Kiambu County, Kenya. *International Academic Journal of Human Resource and Business Administration, 3*(8), 159-171

KBA (2024). State of the Banking Industry Report 2024. Available at: https://www.kba.co.ke/wp-content/uploads/2024/08/State-of-the-Banking-Industry-Report-2024.pdf

Kenya Computer Incident Response Team (KE-CIRT) (2020). *Annual Cybersecurity Incident Report*. Available at: https://www.cirt.go.ke/

Kenya Cybersecurity and Cybercrime Bill (2021).Available at: https://www.icta.go.ke/

Kenya National ICT Survey (2021). *ICT Statistics and Cybersecurity Awareness*. Communications Authority of Kenya. Available at: https://www.ca.go.ke/

Kero, C. A., & Bogale, A. T. (2023). A Systematic Review of Resource-Based View and Dynamic Capabilities of Firms and Future Research Avenues. *International Journal of Sustainable Development & Planning*, *18*(10).

Kirimi, P. N., Kariuki, S. N., & Ocharo, K. N. (2022). Financial soundness and performance: evidence from commercial banks in Kenya. *African Journal of Economic and Management Studies*, *13*(4), 651-667.

Kong, H., Jung, S., Lee, I., & Yeon, S. J. (2023). Information security and organizational performance: Empirical study of Korean securities industry. *ETRI Journal*, *37*(2), 428-437.

Kong, H.-K., Kim, T.-S., & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. *Journal of Intelligent Manufacturing*, *23*(4), 941–953. https://doi.org/10.1007/s10845-010-0402-7

Kori, B. W., Muathe, S., & Maina, S. M. (2020). Financial and non-financial measures in evaluating Performance: the role of strategic intelligence in the context of commercial banks in Kenya. *International Business Research*, *13*(10), 130-130.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, *23*, 361-373.

Kyere, M., & Ausloos, M. (2021). Corporate governance and firms financial performance in the United Kingdom. *International Journal of Finance & Economics*, *26*(2), 1871-1885.

Lubis, N. W. (2022). Resource based view (RBV) in improving company strategic capacity. *Research Horizon*, *2*(6), 587-596.

Mardessi, S. M. (2021). The effect of audit committee characteristics on financial reporting quality: The moderating role of audit quality in the Netherlands. *Corporate ownership and control*, *18*(3), 19-30.

Matemane, R., Denhere, V., Mokabane, M., & Ojeyinka, T. A. (2024). Cybersecurity Risk Disclosure, Board Characteristics, and Firm Performance in the Fourth Industrial Revolution Era: Evidence from an Emerging Economy. *African Finance Journal*, *26*(1), 34-53.

McKinsey Global Surveys (2021): A year in review. Available at ; https://www.mckinsey.com/~/media/mckinsey/featured%20insights/mckinsey%20global%20surveys/mckinsey-global-surveys-2021-a-year-in-review.pdf

Meckling, W. H., & Jensen, M. C. (1976). Theory of the Firm. *Managerial Behavior, Agency Costs and Ownership Structure*.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American journal of sociology*, *83*(2), 340-363.

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, *17*(4), 56–82.

Mukaila, K. A., Sahnun, L., & Oladele, T. O. (2022). Effect of management support for change and employee engagement on employee performance in selected hospitals in Abuja, Nigeria. *International Journal of Economics and Development Policy*, 5(2), 1-21.

Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International review of financial analysis*, *81*, 102103.

Mwim, E. N., & Mtsweni, J. (2022, July). Systematic review of factors that influence the cybersecurity culture. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 147-172). Cham: Springer International Publishing.

Mwim, E. N., Mtsweni, J., & Chimbo, B. (2023, July). Factors Associated with Cybersecurity Culture: A quantitative study of Public E-health hospitals in South Africa. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 129-142). Cham: Springer Nature Switzerland.

Ngaruiya, J., Obi, P., & Mathuva, D. (2022, August). The Effect of Changes in Interest Rate Regulation on the Financial Performance of Banks in Kenya. In *International Workshop on Enterprise Applications, Markets and Services in the Finance Industry* (pp. 68-81). Cham: Springer International Publishing.

Obade, S. (2021). *Corporate Governance: Insider Trading Perspective in Kenya* (Doctoral dissertation, University of Nairobi).

Obogi, M. N., & Kiarie, F.(2019) Effect of Corporate Top Management Support on Project Performance in Selected State Corporations in Kenya. *International Journal of Business & Management, 7*(7),154-166.

Okubo, F. A., Wachiuri, E., & Nyaberi, D. (2024). Facility Security Management and Performance of Ministry of Roads and Transport in Kenya. *International Journal of Social Sciences Management and Entrepreneurship (IJSSME)*, *8*(3).

Oluoch, C. O. (2022). *Effects of Information Technology on Internal Auditing in Commercial Banks in Kenya* (Doctoral dissertation, University of Nairobi).

Oussii, A. A., & Boulila, N. (2021). Evidence on the relation between audit committee financial expertise and internal audit function effectiveness. *Journal of Economic and Administrative Sciences*, *37*(4), 659-676.

Peters, B. G. (2022). Institutional theory. In *Handbook on theories of governance* (pp. 323-335). Edward Elgar Publishing.

Potrac, P., Jones, R. L., & Nelson, L. (2014). Interpretivism. In *Research methods in sports coaching* (pp. 31-41). Routledge.

Raimo, N., Vitolla, F., Marrone, A., & Rubino, M. (2021). Do audit committee attributes influence integrated reporting quality? An agency theory viewpoint. *Business Strategy and the Environment*, *30*(1), 522-534.

Ropem, J. (2024). Influence of cybersecurity training programs on employee behavior in corporate environments in Kenya. *American Journal of Computing and Engineering*, *7*(2), 14-26.

Roustapisheh, N., & Yazdizadeh, H. (2022). Effects of top management support, technological skills, and capabilities on entrepreneurship and organizational performance. *International Transaction Journal of Engineering Management and Applied Sciences and Technologies*, *10*, 17.

Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson.

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, *27*(4), 1049-1071.

Sobh, R., & Perry, C. (2006). Research design and data analysis in realism research. *European Journal of marketing*, *40*(11/12), 1194-1209.

Statista (2024), Number of online crimes reported in Kenya from 2018 to 2022. Available at: https://www.statista.com/statistics/1278764/number-of-online-crimes-reported-in-kenya/

Suddaby, R. (2010). Challenges for institutional theory. *Journal of management inquiry*, *19*(1), 14-20.

Sutton, A., & Tompson, L. (2024). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, 104110.

Teoh, C. S., & Mahmood, A. K. (2017, July). National cyber security strategies for digital economy. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.

The National KE-CIRT/CC. (2025). *Cybersecurity Report October- December 2024*. https://ke-cirt.go.ke/wp-content/uploads/2025/01/2024-25-Q2-Cyber-Security-Report.pdf

UNCTAD (2020). *Cybersecurity Capacity in Africa*. United Nations Conference on Trade and Development. Available at: https://unctad.org/webflyer/cybersecurity-capacity-africa

Usman, A., Che-Ahmad, A., & Abdulmalik, S. O. (2024). The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: a Conceptual Review. *Revista de Gestão Social e Ambiental*, *18*(6), e05691-e05691.

Vavrek, R., Bečica, J., Papcunová, V., Gundová, P., & Mitríková, J. (2021). Number of financial indicators as a factor of multi-criteria analysis via the TOPSIS technique: A municipal case study. *Algorithms*, *14*(2), 64.

Willmott, H. (2015). Why institutional theory cannot be critical. *Journal of Management Inquiry*, *24*(1), 105-111.

World Economic Forum (2022). *Global Risks Report 2022*. World Economic Forum. Available at: https://www.weforum.org/reports/global-risks-report-2022

Zahra, S. A. (2021). The resource-based view, resourcefulness, and resource management in startup firms: A proposed research agenda. *Journal of Management*, *47*(7), 1841-1860.

APPENDICES

Appendix I: Introduction Leteer

Eric Mutunga Ngei
Master of Business Administration (MBA) Candidate
Strathmore University

Dear Respondent,

RE: REQUEST FOR PARTICIPATION IN A STUDY

My name is Eric Mutunga Ngei, and I am currently pursuing a Master of Business Administration (MBA) degree at Strathmore University. As part of the requirements for the completion of my degree, I am conducting research on the topic: "The Effect of Cybersecurity Culture on the Financial Performance of Kenyan Commercial Banks: Moderated by Audit Committee Characteristics."

This study aims to investigate the influence of cybersecurity culture on the financial performance of Kenyan commercial banks, particularly focusing on how audit committee characteristics might moderate this relationship. Your insights and perspectives as a key individual in your organization would be invaluable for this research. The questionnaire will ask questions related to your organization's cybersecurity practices, audit committee characteristics, and the bank's financial performance. Please rest assured that all information provided will be treated with the utmost confidentiality and will solely be used for academic purposes. Participation is entirely voluntary, and you may choose to withdraw at any point during the process. No personal identifiers will be used in any publication of the study results, and your responses will remain anonymous.

If you have any questions or require further clarification about the study, please feel free to contact me directly at eric.ngei@gmail.com.

Thank you for considering this request. I look forward to your positive response.

Yours sincerely,
Eric Mutunga Ngei
+254 720695877

Appendix II: Research Questionnaire

The study below aims to collect your opinion as an employee on aspects of cybersecurity culture and its effect on financial performance in commercial banks. The data collected from this study will provide insights into the level of influence that cybersecurity culture has on the performance of commercial banks. The confidentiality of the data collected will be always maintained.

This questionnaire will take approximately 10 minutes to complete.

Section One: Demographic Data

1. Gender: Male [ ] Female [ ]
2. Age: Below 30 years [ ] 31-40 years [ ] 41 – 50 years [ ] Above 50 years [ ]
3. Level of Education: Diploma [ ] Undergraduate [ ] Postgraduate [ ]
4. Years worked: Below 1 year [ ] 1 – 5 years [ ] 6 – 10 years [ ] 11 – 15 years [ ] Above 15 years

Section Two: Cyber Security Culture and Financial Performance

To what extent do you agree with the following statements about cyber security culture in your organization, rating from strongly agree, agree, neither agree nor disagree, disagree, strongly disagree?

Where; 1= strongly disagree; 2 = disagree; 3 = neither agree nor disagree; 4 = agree; and 5 = strongly agree

Top Management Support

Statements	**1**	**2**	**3**	**4**	**5**
Top management provides sufficient resources for cybersecurity initiatives in the bank which reduces the likelihood of financial losses from cyberattacks					
Senior leadership actively participates in cybersecurity training programs.					
There is clear communication from top management on the importance of cybersecurity culture leading to better financial outcomes by avoiding fines, legal issues, and loss of customer trust.					

Top management staff consider cybersecurity an important organizational priority which enhances financial performance.					
Top management consistently supports initiatives aimed at improving the bank's cybersecurity posture reducing the financial impact of potential breaches					
Top management's commitment to cybersecurity is visible and evident to all employees which supports the bank's long-term financial stability and growth.					

Information security policy

Statements	**1**	**2**	**3**	**4**	**5**
The bank has a well-defined and comprehensive information security policy which minimizes cybersecurity risks, preventing financial losses from data breaches or fraud					
The information security policy is regularly reviewed and updated to reflect emerging cybersecurity threats which reduces the likelihood of costly security incidents					
The information security policy is easily accessible to all employees reducing the risk of breaches that could lead to financial losses					
The policy on cybersecurity is strictly enforced within the bank to mitigate potential risks.					
I am familiar with the organization's policies relating to cybersecurity and the resulting consequences for non-compliance					
Compliance to cybersecurity policy has improved the bank's cybersecurity readiness and minimizes risks and protects its financial performance from potential losses					

Cybersecurity training

Statements	1	2	3	4	5
Employees in the bank regularly receive training on cybersecurity best practices.					

The bank offers cybersecurity training that is relevant to the specific needs of different departments.					
Cybersecurity training programs are mandatory for all staff in the bank.					
Cybersecurity training has helped employees improve their awareness of cyber threats to prevent attacks before they escalate.					
Up-to-date training ensures that employees are prepared to defend against the latest cybersecurity threats, reducing the risk of financial losses					
My organization's cybersecurity team ensures that training is specialized and consistently updated, directly improving the bank's ability to protect itself from financial risks					

Audit Committee Characteristics

Statements	1	2	3	4	5
The audit committee has sufficient expertise in cybersecurity and IT risk management to an effectively identify, assess, and mitigate cybersecurity risk					
The audit committee members possess relevant skills and knowledge to address cybersecurity risks effectively.					
By staying informed about emerging cybersecurity threats, the audit committee can implement proactive measures to prevent security incidents that could lead to financial losses.					
Most members of the audit committee are independent which reduces the likelihood of security oversights or ineffective policies that could negatively impact financial performance.					
Independent decision-making by the audit committee ensures that cybersecurity risks are managed based on their financial and operational impact, rather than short-term managerial interests.					
Audit committee members maintain an objective stance when addressing cybersecurity challenges, ensuring that cybersecurity strategies are designed to minimize financial risk					

Financial Performance

Statements	1	2	3	4	5
The bank has experienced an improvement in profitability over the last year.					
The bank has maintained a strong profit margin despite market challenges.					
The bank's asset management has been efficient in contributing to financial success.					
The cost-to-income ratio has improved over the last year.					
The bank is in a stable financial position to handle economic fluctuations.					
The bank consistently achieves its profitability targets.					

Appendix III: Data collection sheet

Bank Name……

ITEM/Financial Year	2021/2022	2022/2023	2023/2024	Average
Return on Assets (ROA)				

Appendix IV: Ethical Approval

Strathmore UNIVERSITY

2nd April 2025

Mr Ngei Eric,
eric.ngei@strathmore.edu

Dear Mr Ngei,

RE: Effect of Cybersecurity Culture on Financial Performance of Kenyan Commercial Banks: Moderated by Audit Committee Characteristics

This is to inform you that SU-ISERC has reviewed and **approved** your above SU-masters proposal. Your application reference number is **SU-ISERC2766/25.** The approval period is from **2nd April 2025 to 1st April 2026.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

Mr Ambrose Rachier,
Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu

Appendix V: NACOSTI Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 102414

Date of Issue: 08/April/2025

RESEARCH LICENSE

This is to Certify that Mr.. Eric Mutunga Ngei of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: EFFECT OF CYBERSECURITY CULTURE ON FINANCIAL PERFORMANCE OF KENYAN COMMERCIAL BANKS: MODERATED BY AUDIT COMMITTEE CHARACTERISTICS for the period ending : 08/April/2026.

License No: NACOSTI/P/25/417909

102414

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions