African Journal of Emerging Issues
Peer reviewed | Double blind | Interdisciplinary

African Journal of Emerging Issues (AJOEI)
Online ISSN: 2663 - 9335
Available at: https://ajoeijournals.org

STRATEGIC MANAGEMENT

STRATEGIC IMPLEMENTATION OF SECURITY MEASURES ON COMPETITIVE ADVANTAGE FOR SMALL AND MEDIUM ENTERPRISES IN KAMUKUNJI SUB- COUNTY

[*1]Hassan Adan Hassan & [2]Dr. Martin Kimemia

[1]Master Student, Department of Business and Economics, Mount Kenya University, Kenya

[2]Supervisor, Department of Business and Economics, Mount Kenya University, Kenya

***Email of the Corresponding Author: hassalabas@gmail.com**

Publication Date: May 2026

ABSTRACT

Purpose of the Study: This study examined the influence of strategic implementation of security measures on the competitive advantage of SMEs in Kamukunji Sub-County.

Statement of the Problem: SMEs in Kamukunji Sub-County face theft, vandalism, fraud, and cybercrime, which disrupt operations, increase costs, and weaken customer trust. Many SMEs also lack adequate resources and technical capacity to implement effective security systems.

Methodology: The study was anchored on the Resource-Based View Theory and adopted a descriptive design with cross-sectional and correlational approaches. The target population was 2,890 SME owners, employees, and customers, from which 353 respondents were selected using stratified random sampling. Data were collected using semi-structured questionnaires and analyzed using SPSS and Microsoft Excel through descriptive statistics, Pearson correlation, and OLS regression.

Findings: The findings showed that respondents perceived security measures as important in enhancing customer trust, employee confidence, operational stability, and organizational performance. Nevertheless, the direct relationship between security adoption and competitive advantage was weak and statistically insignificant.

Conclusion: The study concluded that security measures are important enabling factors for SMEs, but they do not independently guarantee competitive advantage unless integrated with wider business strategies.

Recommendation: The study recommended that SMEs adopt integrated, practical, and cost-effective physical and digital security strategies supported by employee training and institutional support.

Keywords: *Strategic Implementation, Security Measures, Competitive Advantage, Small and Medium Enterprises, Kamukunji Sub- County*

INTRODUCTION

In the twenty-first century, extraordinary leadership challenges persist to the extent that scholars and practitioners agree that conventional leadership styles are increasingly ineffective in modern businesses (Armstrong & Armstrong, 2021; Burnes, 2017; Northouse, 2019). As time progresses, contemporary organizations encounter mounting challenges, including a multigenerational workforce, heightened human capital competitiveness, and the volatility and uncertainty caused by unanticipated events and ever-changing consumer demands (Armstrong & Armstrong, 2021). Kouzes and Posner (2011) argue that leaders must always be willing to adopt the mindset of a learner, since extraordinary circumstances necessitate equally extraordinary shifts in approach, including in leadership practice. It is therefore more important than ever for organizations to provide a psychological sanctuary in which employees can seek support whenever the need arises (Yukl, 2013). This new leadership reality calls for leaders defined not by their job titles or a single problem-solving approach, but by the qualities they bring to their work, including emotional intelligence, placing others ahead of oneself, ethical conduct, and a concern for the common good (Drucker, 2015; Goleman et al., 2013). Such leaders, according to George (2003), are those who go beyond the bottom line, demonstrating the tenets of authenticity and credibility in their conduct (Walumbwa et al., 2008; Kouzes & Posner, 2011).

Examining leadership within the context of diversity is crucial for understanding what constitutes authentic and credible leadership. As cited in Burnes (2017), diversity encompasses distinctions among people based on demographics, economic status, and abilities. Current leadership research has often been skewed toward western organizations, and incorporating diversity into the research would help practitioners contextualize leadership more effectively in varied settings (Burnes, 2017). Demographic data has periodically been employed to investigate the concept of leadership. Eagly (2005) highlights that gender differences in leadership have continued to attract research interest, particularly with respect to preferred leadership styles, with men tending toward agentic transactional styles and women favoring more accommodative and relational approaches.

Concepts such as age have also proven to be intriguing, with scholars presenting arguments on crystallized cognitive ability, which is believed to be acquired over time and is closely linked to age (Northouse, 2019). Experience closely related to tenure has also been studied, revealing a meaningful relationship between the type of leadership applied, whether directive leadership for

less experienced employees or supportive leadership for more experienced ones who require less structure (Avolio, 1999; Northouse, 2019). Lastly, faith, also referred to as religion or spirituality, can substantively influence a leader's personal philosophy and value system (Yukl, 2013). This study aims to use demographic data, including age, gender, seniority, tenure, and faith, to determine how these variables affect authenticity.

STATEMENT OF THE PROBLEM

The implementation of security measures has become increasingly important for the sustainability and competitiveness of small and medium enterprises (SMEs), particularly in high-risk urban business environments such as Kamukunji Sub-County. SMEs in the area continue to face growing threats from theft, vandalism, fraud, and cybercrime, which negatively affect operational efficiency, customer trust, employee productivity, and overall business performance. Despite the growing importance of security, many SMEs lack adequate resources, technical expertise, and strategic frameworks to implement effective physical and cybersecurity measures.

Ideally, security measures should not only protect business assets but also enhance customer confidence, improve employee morale, reduce operational losses, and strengthen market positioning. Effective security systems can therefore serve as a strategic tool for achieving competitive advantage and long-term business sustainability. National policy frameworks, including the Micro and Small Enterprises Policy (2012) and Kenya Vision 2030, emphasize the importance of a secure business environment in promoting enterprise growth and investment.

Although several studies have examined security challenges facing SMEs, most existing research focuses on security from a risk management and compliance perspective, with limited attention given to security as a strategic driver of competitiveness. There is insufficient empirical evidence on how security measures influence customer trust, employee perceptions, operational performance, and competitive positioning among SMEs operating in high-risk commercial environments. This presents a significant knowledge gap. Therefore, this study seeks to examine the influence of security measures on the competitiveness of SMEs in Kamukunji Sub-County, with the aim of generating insights that can help reposition security from a cost burden to a strategic value-adding function that supports business resilience, sustainability, and growth.

PURPOSE OF THE STUDY

The purpose of this study was to examine the strategic implementation of security measures on a competitive advantage for SMEs in Kamukunji Sub County

Specific Objectives

To assess the influence of security measures on competitive advantage of SMEs in Kamukunji Sub County

LITERATURE REVIEW

This section reviews the theoretical and empirical literature related to the influence of security measures on the competitiveness of small and medium enterprises (SMEs). It begins by presenting the theory guiding the study, followed by a review of empirical literature on security measures and their relationship with SME competitiveness. The section further examines literature on physical and cybersecurity practices, operational efficiency, customer trust, and business sustainability among SMEs. Finally, the section presents the conceptual framework illustrating the relationship between the independent and dependent variables of the study.

THEORETICAL REVIEW

The theoretical review presents the theory that anchors the study and explains how the implementation of security measures may influence the competitiveness of small and medium enterprises (SMEs). The study is guided by the Resource-Based View (RBV) Theory, which provides a useful foundation for understanding how organizations can achieve competitive advantage through the effective utilization and protection of valuable resources and capabilities. The theory emphasizes that strategic resources such as business information, customer trust, operational systems, and organizational knowledge can contribute to sustained competitiveness when adequately secured and managed. In the context of SMEs, the implementation of physical and cybersecurity measures helps protect critical assets, enhance operational efficiency, strengthen customer confidence, and improve overall business performance.

Resource-Based View (RBV) Theory

The Resource-Based View (RBV) Theory was developed by Jay Barney in 1991 to explain how organizations achieve and maintain competitive advantage through the effective use of internal

resources and capabilities. The theory builds on earlier ideas by Edith Penrose (1959) and Birger Wernerfelt (1984), who emphasized that the resources owned and controlled by a firm play a major role in determining its growth and performance. According to the RBV theory, businesses are more likely to succeed when they possess resources that are valuable, rare, difficult to imitate, and not easily replaced by competitors.

The theory is relevant to this study because it helps explain how security measures can contribute to the competitiveness of SMEs operating in Kamukunji Sub-County. SMEs in the area operate in an environment characterized by challenges such as theft, vandalism, fraud, and cybercrime. These security threats often lead to financial losses, interruptions in business operations, and reduced customer confidence. The RBV theory suggests that businesses that invest in effective security systems are better positioned to protect their valuable assets and maintain stable operations, which can strengthen their competitive position in the market.

In this study, security measures are viewed as strategic resources that support business performance and sustainability. These measures include physical security systems such as CCTV cameras, alarm systems, access control systems, and security personnel, as well as digital security measures such as firewalls, data encryption, antivirus software, and cybersecurity awareness training for employees. When properly implemented, these security practices help businesses minimize risks, reduce operational disruptions, and create a safer business environment for both employees and customers.

The theory further explains that organizations with strong security systems are likely to enjoy better operational efficiency and improved customer trust. Customers are more likely to engage with businesses that demonstrate the ability to protect transactions, personal information, and business operations. Similarly, employees working in secure environments tend to feel safer and more motivated, which can improve productivity and service delivery. These benefits contribute to stronger business performance and enhance the organization's reputation within the market.

The RBV theory also highlights the importance of sustainability and long-term competitiveness. SMEs that continuously invest in and improve their security systems develop capabilities that competitors may find difficult to replicate. For example, businesses with strong cybersecurity systems and trained employees are better prepared to respond to emerging security threats

compared to firms with weak security structures. This ability to adapt and respond effectively to risks can help SMEs remain competitive in rapidly changing business environments. Therefore, the Resource-Based View (RBV) Theory provides a suitable foundation for this study because it demonstrates how security measures can move beyond their traditional protective role and become strategic assets that support operational efficiency, customer confidence, business resilience, and overall competitiveness among SMEs in Kamukunji Sub-County.

EMPIRICAL REVIEW

The empirical literature on security measures and SME competitiveness shows that existing studies have mainly focused on security as a risk management and compliance tool rather than a strategic driver of competitive advantage. Prior research indicates that effective physical and cybersecurity measures contribute to improved operational efficiency, reduced losses, enhanced customer trust, better employee performance, and stronger market positioning. However, despite these established benefits, there remains limited empirical evidence on how SMEs strategically use security to gain competitiveness, particularly in high-risk and densely populated business environments. In particular, a clear research gap exists regarding SMEs operating in Kamukunji Sub-County, where security challenges are prevalent but underexplored in relation to competitive advantage.

Security Measures and Competitive Advantages of SMEs

Security measures are increasingly viewed as a strategic factor that influences the competitiveness of small and medium enterprises (SMEs). From a strategic management perspective, competitiveness is achieved when firms are able to protect their key assets, reputation, and operations from internal and external threats (Hitt et al., 2020). For SMEs, especially those operating in high-risk environments such as Kamukunji Sub-County, security measures serve not only as protective tools but also as enablers of business continuity, customer confidence, and operational stability. Empirical evidence shows that both physical and cybersecurity investments contribute significantly to improved business performance. Physical security systems such as CCTV, alarm systems, and access controls help reduce theft, vandalism, and operational disruptions. For example, reports from the National Police Service (2022) indicate that SMEs in Kamukunji that adopted physical security measures experienced a notable reduction in theft-related losses, leading to improved continuity of operations. Similarly, cybersecurity measures

such as firewalls, encryption, and secure data management systems reduce exposure to cyber threats such as phishing, ransomware, and hacking, thereby protecting business information and customer data.

Studies also show that security influences customer trust and market positioning. According to the European Union Agency for Cybersecurity (ENISA, 2023), SMEs that integrate both physical and digital security systems tend to record higher customer retention rates because clients feel more confident engaging with businesses that protect their data and transactions. In the same way, the Communications Authority of Kenya (2022) reports that SMEs with strong cybersecurity practices experience improved customer loyalty and enhanced brand credibility, giving them a competitive edge in the market. Beyond customer trust, security measures also improve internal organizational performance. Secure working environments enhance employee confidence, reduce stress related to insecurity, and increase productivity. Additionally, reduced losses from theft, fraud, and cyber incidents allow SMEs to redirect resources toward expansion, innovation, and service improvement. The International Finance Corporation (IFC, 2022) further notes that SMEs with strong cybersecurity frameworks experience fewer operational disruptions and improved system uptime, which strengthens overall efficiency and competitiveness.

However, empirical literature also highlights significant barriers to the adoption of comprehensive security systems among SMEs. Financial constraints and limited technical capacity remain major challenges, particularly in developing economies. A report by the World Bank and SME policy studies (2023) indicates that many SMEs in Kenya struggle to allocate sufficient resources for security investments, even though partial adoption of basic measures still results in reduced risk exposure. This suggests that even low-cost security interventions can contribute meaningfully to improved business resilience. Government and institutional support also play an important role in strengthening SME security. In Kenya, initiatives by the National Cybersecurity Strategy (2021), the Communications Authority of Kenya (2022), and the National Police Service have focused on building awareness, improving infrastructure, and supporting SMEs with training programs. Evidence shows that SMEs participating in such programs report reduced vulnerability to cyber threats and improved customer trust, reinforcing the importance of institutional support in enhancing competitiveness.

CONCEPTUAL FRAMEWORK

The conceptual framework presents the relationship between the study variables. It illustrates how security measures, as the independent variable, are expected to influence the competitiveness of small and medium enterprises (SMEs) in Kamukunji Sub-County. In this study, security measures include both physical security (such as CCTV surveillance, alarm systems, and access control) and cybersecurity practices (such as data protection systems, encryption, and cybersecurity awareness).

The dependent variable is SME competitiveness, which is reflected through indicators such as operational efficiency, customer trust, employee performance, and market positioning. The framework assumes that effective implementation of security measures enhances business stability, reduces risks, and strengthens customer and employee confidence, thereby improving overall competitiveness.

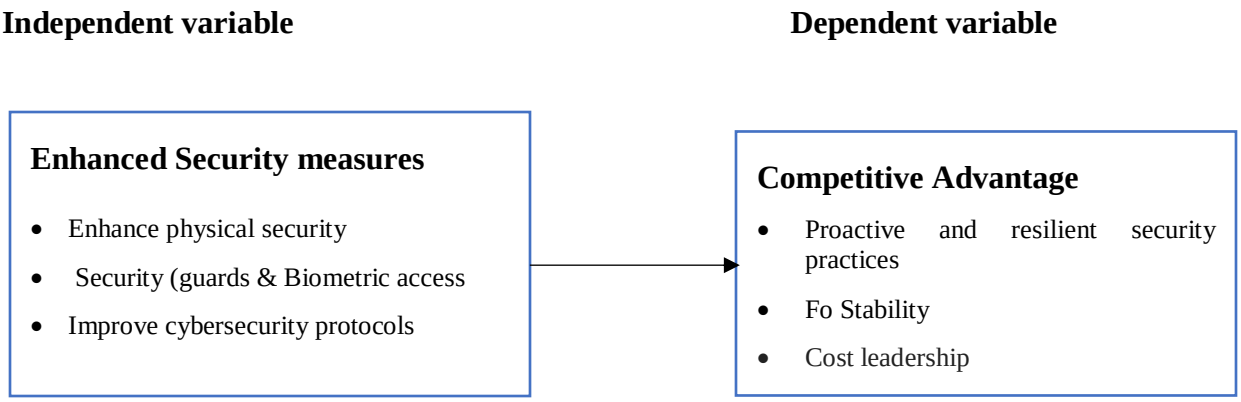

Figure 1: Conceptual Framework

METHODOLOGY

This study adopted a mixed research design using quantitative and qualitative approaches to examine the influence of security measures on the competitiveness of SMEs in Kamukunji Sub-County. A cross-sectional and correlational design was used to collect data at one point in time and determine the relationship between security measures and SME competitiveness. The target population comprised 2,890 respondents, including 256 SME owners, 1,142 employees, and 1,492 customers from Muthurwa Market. A sample of 353 respondents was determined using Yamane's formula and proportionately distributed across the three groups. Stratified random sampling

ensured fair representation, while purposive sampling was used for SME owners with security systems, and simple random sampling was applied to employees and customers. Data were collected using questionnaires, interviews, observation, and documentary review. A pilot study involving 12 respondents from City Market was conducted to refine the instruments. Reliability was tested using Cronbach's Alpha, test-retest, and split-half methods, while validity was ensured through expert review, pre-testing, and alignment with the study constructs. Quantitative data were analyzed using descriptive statistics, Pearson correlation, and multiple regression, while qualitative data were analyzed thematically. Ethical considerations, including informed consent, confidentiality, voluntary participation, and data protection, were observed throughout the study.

RESEARCH FINDINGS

This section presents the findings of the study based on data collected from respondents in small and medium enterprises (SMEs) in Kamukunji Sub-County. The results are organized into descriptive and inferential statistics to provide a clear understanding of the relationship between security measures and SME competitiveness. Descriptive statistics are presented using frequencies, percentages, means, and standard deviations to summarize respondents' views on the study variables. Inferential statistics are presented using correlation and regression analysis to determine the nature and strength of the relationship between security measures and competitive advantage. The respondents rated the study statements using a five-point Likert scale, where 1 represented strongly disagree, 2 disagree, 3 neutral, 4 agree, and 5 strongly agree. This scale was used to measure respondents' perceptions of physical and cybersecurity measures, customer trust, employee perceptions, operational efficiency, and overall competitiveness of SMEs.

DESCRIPTIVE STATISTICS RESULTS

Descriptive statistics were used to summarize respondents' views on the key study variables. The analysis focused on security measures as the key independent variable and the competitiveness of small and medium enterprises (SMEs) as the dependent variable in Kamukunji Sub-County. The results present the extent to which respondents agreed that physical and cybersecurity practices contribute to operational efficiency, customer trust, employee safety, risk reduction, and overall business performance. The findings further indicate respondents' perceptions on how effective implementation of security measures supports business continuity, improves market positioning,

enhances customer confidence, and strengthens the competitive advantage of SMEs operating in high-risk environments.

Assess the Influence of Security Measures Undertaken for Competitive Advantage of SMEs

The results in Table 1 show that most SMEs generally agree that security measures play an important role in strengthening their competitive position. The majority of the statements recorded mean scores above 4.0, indicating a strong level of agreement that security practices contribute positively to business performance and competitiveness.

Table 1: Security Measures Undertaken for Competitive Advantage

	N	Mean	Std. Deviation
Use of advanced security technologies	27	4.52	0.58
Employee training on security protocols	27	4.22	0.974
Investment in physical security infrastructure	27	4.44	0.577
Adoption of digital security measures	27	4.41	0.797
Security measures give a competitive edge	27	4.44	0.751
Collaboration with law enforcement improves business safety	27	3.81	1.272
Real-time monitoring builds customer trust	27	3.85	1.231

The highest-rated aspect was the use of advanced security technologies (M = 4.52, SD = 0.580), suggesting that respondents strongly value modern security tools such as CCTV systems, alarms, and digital surveillance in improving business protection and competitiveness. This is closely followed by investment in physical security infrastructure (M = 4.44, SD = 0.577) and the belief that security measures provide a competitive advantage (M = 4.44, SD = 0.751). These findings show that many SMEs consider physical protection a key foundation for business stability and market success. In addition, adoption of digital security measures (M = 4.41, SD = 0.797) and employee training on security procedures (M = 4.22, SD = 0.974) were also highly rated. This indicates that SMEs understand the importance of not only investing in security systems but also equipping employees with the right knowledge to use them effectively. Together, these efforts help strengthen overall business resilience and competitiveness.

On the other hand, real-time monitoring and its role in building customer trust (M = 3.85, SD = 1.231) and collaboration with law enforcement to improve safety (M = 3.81, SD = 1.272) received

comparatively lower ratings. These mixed responses suggest that some SMEs may not fully experience or consistently benefit from these external security arrangements, or they may view them as less directly impactful on daily business competitiveness. Overall, the findings suggest that SMEs place greater importance on internal security investments as more immediate drivers of competitive advantage, while external partnerships and monitoring systems are seen as supportive but less influential factors.

One Sample Test

The one-sample t-test results in Table 2 indicate that all security-related variables have mean scores that are significantly higher than the test value of 3 (neutral point), suggesting that respondents generally agree that security measures contribute positively to competitive advantage among SMEs.

Table 2: One-Sample Test (Test Value = 3)

One-Sample Test	Test Value = 3					
	T	Df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference Lower	Upper
Use of advanced security technologies	13.609	26	.000	1.519	1.29	1.75
Employee training on security protocols	6.520	26	.000	1.222	.84	1.61
Investment in physical security infrastructure	13.000	26	.000	1.444	1.22	1.67
Adoption of digital security measures	9.175	26	.000	1.407	1.09	1.72
Security measures give a competitve edge	9.993	26	.000	1.444	1.15	1.74
Collaboration with law enforcement improves business safety	3.328	26	.003	.815	.31	1.32
Real-time monitoring builds customer trust	3.595	26	.001	.852	.36	1.34

The strongest statistical significance is observed in use of advanced security technologies ($t = 13.609$, $p < 0.001$, mean difference = 1.519) and investment in physical security infrastructure ($t = 13.000$, $p < 0.001$, mean difference = 1.444). These results show that SMEs strongly perceive modern security systems and physical protection as key contributors to competitiveness, with high levels of confidence reflected in the narrow confidence intervals. Similarly, adoption of digital

security measures (t = 9.175, p < 0.001) and the perception that security measures give a competitive edge (t = 9.993, p < 0.001) also show strong positive deviations from the neutral point. This confirms that SMEs widely recognize both physical and digital security as essential strategic tools for improving market position and operational resilience.

Although still statistically significant, employee training on security protocols (t = 6.520, p < 0.001) shows a relatively lower mean difference compared to infrastructure and technology-based measures. This suggests that while training is valued, it is not perceived as strongly as physical or technological investments in driving competitiveness. On the other hand, collaboration with law enforcement (t = 3.328, p = 0.003) and real-time monitoring for customer trust (t = 3.595, p = 0.001), though significant, recorded the lowest t-values and mean differences. This indicates that respondents view external security support systems as less influential compared to internal security investments.

CORRELATIONS

Table 3: Correlation Analysis

	Security adoption	**Competitive advantage**	
Security adoption	Pearson Correlation	1	-0.098
	Sig. (2-tailed)		0.625
	N	27	27
Competitive advantage	Pearson Correlation	-0.098	1
	Sig. (2-tailed)	0.625	
	N	27	27
Variables	Correlation (r)	Significance (p)	
Security adoption & competitive advantage	-0.098	0.625s)	

The results in Table 3 show a very weak negative relationship between security adoption and competitive advantage among SMEs (r = -0.098). This indicates that, within the study area of Kamukunji Sub-County, increases in security adoption are not meaningfully associated with improvements in competitive advantage. In addition, the relationship is statistically insignificant (p = 0.625), which is greater than the 0.05 significance level. This means that the observed relationship is not strong enough to be considered real and may have occurred by chance. Overall,

the findings suggest that simply adopting security measures does not automatically lead to a competitive advantage for SMEs. This implies that the effectiveness of security may depend on other factors such as how well it is implemented, integrated into business operations, and perceived by customers and employees.

CONCLUSIONS

The study concludes that although the quantitative results did not establish a statistically significant relationship between security measures and competitive advantage among SMEs, the broader evidence from qualitative insights and secondary data strongly indicates that security remains strategically important. In particular, security measures were found to play a key role in strengthening customer trust, improving employee confidence and productivity, and reducing operational risks, all of which are essential for sustaining long-term business competitiveness in Kamukunji Sub-County.

The absence of a strong statistical relationship may be attributed to measurement limitations, differences in how SMEs implement security measures, and the uneven nature of security challenges across enterprises. Some SMEs may have adopted security practices without fully integrating them into their strategic operations, thereby limiting their observable impact on competitiveness. Overall, the findings suggest that security is not a direct or standalone driver of competitive advantage, but rather a critical enabling factor whose impact depends on effective implementation, organizational context, and integration with broader business strategies. In high-risk environments such as Kamukunji, security therefore remains a necessary but complex component of SME performance and sustainability.

RECOMMENDATIONS

SMEs are encouraged to adopt an integrated security approach that combines both physical measures (such as surveillance systems and secure storage facilities) and digital protections (including strong password policies, cybersecurity awareness, and staff training). This holistic approach would help create stronger and more reliable protection systems capable of reducing both physical and cyber risks.

Business owners should also actively communicate and demonstrate the strategic value of security within their organizations. By promoting security as a key business asset to both employees and

customers, SMEs can strengthen trust, improve customer loyalty, and enhance employee confidence in the workplace.

Government institutions, trade associations, and non-governmental organizations should play a more active role in supporting SMEs through accessible and practical training programs, particularly in cybersecurity awareness and risk management. In addition, public–private partnerships should be strengthened to ease the financial burden of acquiring and maintaining modern security technologies by offering subsidies, tax incentives, or affordable financing options.

Policy frameworks should be improved to provide clear security guidelines, technical support, and minimum-security standards tailored to the needs of SMEs, especially in high-risk areas such as Kamukunji Sub-County. Finally, future researchers should focus on developing more robust measurement tools for assessing the impact of security on competitiveness and explore how factors such as firm size, industry type, and digital maturity influence this relationship over time.

REFERENCES

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120.

Communications Authority of Kenya. (2022). *Cybersecurity report on digital threats in Kenya*. Nairobi: CAK.

DeVellis, R. F. (2017). *Scale development: Theory and applications* (4th ed.). Sage Publications.

European Union Agency for Cybersecurity (ENISA). (2023). *Cybersecurity for SMEs in Europe*. Brussels: ENISA.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Sage Publications.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Pearson.

Hitt, M. A., Ireland, R. D., & Hoskisson, R. E. (2020). *Strategic management: Competitiveness and globalization*. Cengage Learning.

International Finance Corporation (IFC). (2022). *Cybersecurity and SME performance in developing economies*. Washington, DC: World Bank Group.

Kamukunji Sub-County Development Plan. (2022). Nairobi County Government.

Kamukunji Sub-County Economic Report. (2023). *Local economic development report*. Nairobi County Government.

Kenya Cybersecurity Bill. (2022). Government of Kenya.

Kenya National Bureau of Statistics (KNBS). (2023). *Economic survey report*. Nairobi: Government Printer.

Kenya National Cybersecurity Strategy. (2021). *National cybersecurity framework*. Government of Kenya.

Kibera, F. N. (2021). *Business environment and competitiveness in Kenya*. Nairobi University Press.

Kumar, R., & Kumar, U. (2018). Cybersecurity practices in SMEs. *International Journal of Information Security*, 12(3), 45–60.

Mungai, E. (2022). SME security challenges in urban Kenya. *African Journal of Business Management*, 16(4), 112–125.

Muriuki, P. (2021). Physical security systems and business performance in SMEs. *Journal of Entrepreneurship Studies*, 8(2), 55–70.

National Cybersecurity Authority of Kenya. (2023). *Cybersecurity awareness and SME protection report*. Nairobi.

National Police Service. (2022). *Crime and business security report*. Nairobi: Government of Kenya.

OECD. (2021). *Cybersecurity for SMEs: Policy insights*. Paris: OECD Publishing.

Penrose, E. (1959). *The theory of the growth of the firm*. Oxford University Press.

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. Free Press.

Republic of Kenya. (2022). *Ministry of Trade annual report*. Nairobi: Government Printer.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson.

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

Trochim, W., & Donnelly, J. (2008). *The research methods knowledge base*. Atomic Dog Publishing.

UNCTAD. (2022). *Trade and development report: SMEs and global competitiveness*. United Nations.

UNIDO. (2022). *SMEs and sustainable development in East Africa*. United Nations Industrial Development Organization.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171–180.

World Bank. (2023). *SME development and digital security in developing economies*. Washington, DC.