Article

Exploring the Impact of Cybersecurity Threats on Small and Medium Enterprises' Performance: A Case Study of Kajiado County, Kenya

Jacob Neyole * , Saad Minado Okwiri , Nelson Mapema

Posted Date: 5 November 2024

doi: 10.20944/preprints202411.0237.v1

Keywords: cybersecurity threats; cybersecurity infrastructures; small and medium enterprises performance

Article

Exploring the Impact of Cybersecurity Threats on Small and Medium Enterprises' Performance: A Case Study of Kajiado County, Kenya

Saad Okwiri Minado [1], Jacob Neyole [2,*] and Nelson Mapema [3]

[1] Umma University
[2] Umm TVET Institute
[3] Multimedia University
* Correspondence: njacob@tvet.umma.ac.ke

Abstract: Cybersecurity threats pose a significant challenge to the operational resilience and sustainability of Small and Medium Enterprises (SMEs) globally, with distinct implications for regional business ecosystems. This research presents an in-depth investigation into the impact of cybersecurity threats on SMEs within the unique context of Kajiado County, Kenya. Against the backdrop of an increasingly digitized business environment, this study aims to comprehensively assess the challenges SMEs face in mitigating cyber risks and their consequent impact on performance. The research employed a mixed methods approach, combining quantitative and qualitative analyses to elucidate the multifaceted nature of cybersecurity challenges encountered by SMEs in Kajiado County. Utilizing interviews, and document analysis, the study gathered empirical data to identify prevalent cybersecurity threats, their frequency, and the subsequent repercussions on SMEs' operational efficiency, financial stability, and overall performance metrics. Initial findings reveal a diverse spectrum of cybersecurity threats SMEs face in Kajiado County, ranging from phishing attacks and data breaches to ransomware incidents. These threats significantly impede business operations, resulting in financial losses, service delivery disruptions, and customer trust erosion. Moreover, the study examined the cybersecurity measures adopted by SMEs, highlighting the challenges in implementing effective preventive strategies within resource-constrained environments. Notably, the research addresses the identified gap by offering a nuanced understanding of the interplay between cybersecurity threats and SME performance in Kajiado County. The study intends to propose tailored and pragmatic recommendations to fortify SMEs' cybersecurity resilience by contextualizing global best practices within the regional business landscape. The anticipated outcomes of this research endeavor extend beyond academic discourse, aiming to provide actionable insights to SME stakeholders, policymakers, and industry practitioners. The findings aspire to empower SMEs in Kajiado County to enhance their cybersecurity posture, enabling them to navigate the evolving threat landscape more effectively and bolster their long-term sustainability within the digital economy.

Keywords: cybersecurity threats; cybersecurity infrastructures; small and medium enterprises performance

1. Introduction

Small businesses and sized enterprises (SMEs) play an essential role in Kenya's economy, making a meaningful impact on job creation, innovation, and overall economic progress (Amoit Enaga & Naomi Kathula, 2022). As business operations become more digitized and interconnected, SMEs in Kajiado County face both opportunities and risks. The digital revolution has opened up possibilities for growth while also exposing these businesses to cybersecurity challenges (Chege & Wang, 2020).

In the years, there has been a significant increase in the number and complexity of cyber-attacks targeting small and medium-sized enterprises (SMEs (Mantha et al., 2021). These attacks come in forms like phishing, ransomware, and data breaches. The interconnected nature of today's business landscape means these threats have far-reaching consequences beyond compromising data. They can severely impact SMEs' efficiency and financial stability (Rawindaran et al., 2023).

An increasing reliance on digital technologies and the Internet characterizes modern business operations and has altered the business environment for companies in many industries (Henderson, 2023). The everyday life of small and medium-sized enterprises (SMEs) is increasingly dependent on digital tools and online platforms. The efficiency benefits, cost-effectiveness, and improved connectivity afforded by digital technology drive this dependency increase. Companies across industries are leveraging the power of the Internet to expedite procedures and increase their reach, from communications and collaboration to marketing and sales (Hamed Taherdoost, 2022).

In particular, SMEs are navigating this digital transformation to stay competitive and meet evolving consumer expectations. Cloud-based services, e-commerce platforms, and digital communication tools have become integral components of SMEs' operational frameworks (Chege & Wang, 2020). The shift towards online business operations optimizes efficiency and opens up new avenues for market access, customer engagement, and innovation (Amoit & Kathula, 2022).

As digital technologies become more widely used, cybersecurity risks rise. Due to increased connectivity, small and medium-sized businesses are becoming increasingly vulnerable to ransomware attacks, phishing scams, and data breaches. As a result, reaping the benefits of digitalization for business operations necessitates an understanding of and commitment to mitigating these cybersecurity risks (Borah et al., 2022). The interplay of advantages and disadvantages emphasizes the need to thoroughly analyze the effects of this increased reliance on digital technologies in the context of SMEs, especially in areas like Kenya's Kajiado County.

The context of Kajiado County provides a unique lens through which to examine these dynamics. As a region characterized by a burgeoning SME sector, its vulnerabilities to cybersecurity threats underscore the urgency of understanding the specific challenges SMEs face in this locale. Government initiatives and regulatory frameworks aimed at cybersecurity in Kenya add another layer of complexity to this landscape.

The research delves into the intricate relationship between cybersecurity threats and how small and medium-sized enterprises (SMEs) perform in Kajiado County. It sheds light on the specific difficulties they encounter. By thoroughly investigating the cybersecurity environment in this particular setting, the study offers practical insights to help SMEs in Kajiado County adapt and thrive securely and sustainably in the digital world.

1.2. Problem Statement

The growing prevalence of cyber security threats poses a serious challenge to the performance and sustainability of small and medium enterprises (SMEs) in Kajiado County, Kenya. As businesses increasingly rely on digital technology and the internet for their operations, the risk of cyberattacks becomes more pronounced. Small and medium-sized businesses, which are a vital sector of the Kenyan economy, face the risk of data breaches, ransomware, and other malicious activities that can compromise sensitive information and cause disruption. essential business processes.

Despite the looming threat of cyberattacks, there exists a significant gap in understanding the specific nature and impact of cybersecurity challenges faced by SMEs in Kajiado County. This lack of tailored insights impedes the development and implementation of effective cybersecurity strategies specifically designed for the unique context of these enterprises. the knowledge gap is further compounded by the ever-evolving tactics employed by cybercriminals, necessitating a continuous and adaptive approach to cybersecurity defense. Furthermore, the economic significance of SMEs in Kajiado County underscores the potential gravity of cyber incidents.

A successful cyberattack not only jeopardizes the confidentiality, integrity, and availability of critical business data but also undermines the financial stability and operational continuity of these enterprises. The absence of a comprehensive understanding of the cybersecurity landscape in Kajiado County further exacerbates the vulnerability of SMEs to these threats. Addressing this pressing issue demands a thorough investigation into the types, frequency, and impact of cybersecurity threats on SMEs in Kajiado County. By bridging the existing knowledge gap, this research endeavored to provide actionable insights that empower SMEs to fortify their cybersecurity defenses and safeguard their operational performance in an increasingly digitalized business environment.

1.3. Objectives of the Study

The general objective of the study was to explore the impact of cybersecurity threats on small and medium enterprises' performance. The specific objectives were to:

(i) Clearly define and categorize various types of cybersecurity threats faced by SMEs in Kajiado County.
(ii) Evaluate the direct and indirect consequences of cybersecurity incidents on the operational efficiency and financial stability of SMEs.
(iii) Quantify the frequency and intensity of identified cybersecurity threats to establish a baseline understanding.
(iv) Investigate existing cybersecurity measures implemented by SMEs in Kajiado County, ensuring that the research scope aligns with available resources.
(v) Propose practical recommendations and strategies for SMEs in Kajiado County based on synthesized findings, ensuring they address the specific challenges faced by these enterprises in the local context.

1.4. Study Justification

The main justification for conducting this research lies in the imperative need to address the burgeoning and evolving challenges posed by cybersecurity threats to Small and Medium Enterprises (SMEs) in Kajiado County, Kenya. As digitalization becomes increasingly integral to business operations, the vulnerabilities of SMEs to cyber-attacks escalate, jeopardizing not only their sensitive data but also their operational efficiency and financial stability. This research strategically aligns with the contemporary business landscape, where the reliance on digital technologies is pervasive.

By delving into the specific context of Kajiado County, the study recognizes the unique challenges faced by SMEs in this region, contributing localized insights that can inform tailored cybersecurity strategies. Furthermore, as SMEs play a pivotal role in Kenya's economic development, enhancing their cybersecurity resilience becomes a strategic imperative for sustained growth. The findings of this research are anticipated to not only fill a crucial knowledge gap but also provide practical recommendations that can empower SMEs in Kajiado County to navigate the intricate cybersecurity landscape, fostering their long-term sustainability and contributing to the overall economic resilience of the region.

1.5. Limitations of the Research

(i) The study's findings are contingent on the representativeness of the selected sample of SMEs in Kajiado County. Limitations may arise if certain subsectors or demographics are underrepresented, impacting the generalizability of the results.
(ii) The reliance on surveys, interviews, and document analysis as primary data collection methods may introduce potential biases. Respondents may underreport cybersecurity incidents due to confidentiality concerns, and the accuracy of historical data and documents could be subject to limitations.
(iii) The dynamic nature of cybersecurity threats implies that the research findings are time-sensitive. The study's outcomes may not fully capture emerging threats or changes in SMEs' cybersecurity practices that occur after the research period.
(iv) The research primarily focuses on identifying and understanding the impact of cybersecurity threats. While recommendations for enhanced resilience are provided, the study may not comprehensively explore the effectiveness of specific mitigation strategies adopted by SMEs.

2. Literature Review

The literature highlights the increasing importance of cybersecurity in SMEs around the world. Research highlights the growing frequency and complexity of cyber threats that affect SMEs. It also highlights SMEs' unique vulnerabilities due to their limited resources and lack of expertise. In this discussion, we discuss the challenges of implementing strong cybersecurity in the context of SMEs' operational limitations.

2.1. Cybersecurity Landscape in Kenya

Kenya's cybersecurity landscape is rapidly evolving, driven by the country's growing digital economy and increasing reliance on technology. The country faces several cybersecurity challenges, including a lack of skilled cybersecurity professionals, inadequate cybersecurity awareness, and outdated cybersecurity infrastructure (Sambuli et al., 2016). However, the Kenyan government is taking steps to address these challenges and improve the country's cybersecurity posture.

A comprehensive review of the cybersecurity landscape in Kenya reveals the country's proactive approach to addressing cyber threats. Government initiatives, such as the National Cybersecurity Strategy, are examined, along with regulatory frameworks designed to safeguard businesses (Leonard et al., 2020). Among the threats are instances of malware, a form of software specifically crafted to inflict harm upon computer systems.

Malware can be engineered to carry out diverse malevolent actions, such as data theft, file encryption, or the disruption of normal operations within a computer system (Okuku et al., 2015). In addition to malware, phishing attacks pose a substantial risk to cybersecurity in Kenya. These attacks involve deceptive attempts to manipulate users into divulging sensitive information, including passwords or credit card numbers. Typically orchestrated through emails or websites that mimic legitimate organizations, phishing attacks exploit users' trust to gain unauthorized access to confidential data (Sambuli et al., 2016).

Ransomware represents another formidable cybersecurity challenge in Kenya. This malicious software encrypts a victim's files, rendering them inaccessible until a ransom is paid. The consequences of ransomware attacks can be severe for businesses, causing disruption to operations and preventing access to critical data (Leonard et al., 2020). The coercive nature of ransomware often leads to difficult decisions for organizations facing such attacks (Kiboi, 2015).

Denial-of-service (DoS) attacks further compound the cybersecurity landscape in Kenya. These attacks involve deliberate efforts to overwhelm a computer system or network with excessive traffic, rendering it inaccessible to legitimate users (Pawar & Palivela, 2022). The motivations behind DoS attacks can range from disrupting businesses and launching other cyberattacks to extorting money from the victims. The potential consequences of these attacks underscore the critical need for robust cybersecurity measures to safeguard digital infrastructure and mitigate the impact on businesses and individuals in Kenya (Ikovo, 2018).

The country grapples with a range of cybersecurity challenges that collectively pose significant risks to businesses and individuals. One pressing issue is the shortage of skilled cybersecurity professionals within the country (Okuku et al., 2015). The inadequacy of qualified experts makes it challenging for businesses to secure the necessary talent to safeguard their systems and sensitive data effectively. This scarcity exacerbates the overall vulnerability of organizations to cyber threats, hindering their ability to implement robust security measures (Kiboi, 2015).

In addition, a substantial portion of the population lacks sufficient awareness of the diverse cybersecurity threats they face. This lack of awareness renders individuals more susceptible to various cyber-attacks, particularly phishing and other social engineering techniques (Mwania Kasyuma, 2016). Without a comprehensive understanding of these threats, individuals may inadvertently compromise their personal information and fall victim to cybercriminal activities. Furthermore, a prevalent issue contributing to Kenya's cybersecurity challenges is the presence of outdated cybersecurity infrastructure in many businesses (Okuku et al., 2015).

Numerous enterprises in the country rely on cybersecurity systems that are not equipped to handle the latest and most sophisticated threats. This outdated infrastructure creates a vulnerability gap, leaving businesses exposed to evolving cyber risks (Thompson, 2023). The inability of existing systems to keep pace with emerging threats underscores the critical need for businesses to invest in and update their cybersecurity infrastructure to enhance overall resilience against cyber threats in the Kenyan landscape (Mwangi & Brown, 2015).

2.2. The Kenya Government's Initiative Against Cyber Threats

The Kenyan government is actively addressing the cybersecurity challenges faced by the country through a series of strategic initiatives (Victor Chitechi et al., 2018). Central to these efforts is the National Cybersecurity Strategy 2022-2027, a comprehensive plan to enhance Kenya's overall cybersecurity posture. The strategy encompasses multifaceted goals, including the promotion of cybersecurity awareness, the development of a skilled cybersecurity workforce, and the enhancement of critical cybersecurity infrastructure (Thompson, 2023).

An integral component of the government's cybersecurity framework is the Kenya Computer Emergency Response Team (CERT), a specialized agency tasked with responding to cybersecurity incidents (Mwangi & Brown, 2015). Functioning as a pivotal arm in the country's cybersecurity defense, the Kenya CERT plays a crucial role in providing technical assistance to businesses and organizations affected by cyberattacks. This responsive approach contributes to mitigating the impact of cyber threats on various sectors (Sutherland, 2018).

In parallel, the government has introduced the Ajira Digital Talent Initiative, a program designed to address the shortage of skilled cybersecurity professionals in Kenya (Morgante & Fabian Wallace Stephens, 2021). Through government funding, this initiative focuses on equipping Kenyans with essential cybersecurity skills. By doing so, the Ajira Digital Talent Initiative not only seeks to bolster the nation's cybersecurity workforce but also aligns with broader national objectives related to digital skills development (Barasa & Kiiru, 2023; Ngetich & Migosi, 2023).

Collectively, these cybersecurity initiatives underscore the government's commitment to fostering a resilient and secure digital environment in Kenya. By strategically combining awareness-building, incident response capabilities, and targeted skill development, the government aims to strengthen the nation's ability to withstand and combat evolving cyber threats. These initiatives not only reflect a proactive stance in addressing current challenges but also demonstrate a forward-looking approach to cybersecurity in Kenya.

2.3. Empirical Analysis Studies on SMEs and Cybersecurity

Existing research provides valuable insights into the impact of cybersecurity threats on SMEs. Studies from diverse regions underscore commonalities in challenges faced by SMEs, including financial implications, reputational damage, and operational disruptions. Numerous empirical studies have explored the impact of cybersecurity threats on Small and Medium Enterprises (SMEs) across different regions, shedding light on the multifaceted nature of these challenges. The table below summarizes the key studies and their findings about the subject.

Empirical Analysis	Key Findings	References
1. Impact of Cybersecurity Breaches on SMEs' Finances	Substantial financial strain due to costs associated with data recovery, system restoration, and potential legal consequences.	(Amrin, 2014; Ravi, 2022)
2. Effectiveness of Employee Training Programs	Targeted training improves employees' awareness of cyber threats, reducing the likelihood of falling victim to phishing attacks and other social engineering tactics.	(Bada, & Nurse, 2019)

3. Regulatory Compliance and Cybersecurity Practices	Positive correlation between adherence to industry-specific cybersecurity regulations and implementation of robust security measures.	(Kabanda et al., 2018; Antunes et al., 2021)
4. Role of Leadership in Cybersecurity Preparedness	Engaged leadership positively correlates with the implementation of comprehensive cybersecurity policies, emphasizing a top-down approach.	(Ravi, 2022)
5. Cybersecurity Insurance Uptake and Risk Mitigation	The adoption of cybersecurity insurance is linked to increased investment in proactive risk management practices, such as regular vulnerability assessments.	(Sullivan, & Nurse, 2021)
6. Effectiveness of Multi-Factor Authentication	Multi-factor authentication significantly reduces unauthorized access, showcasing the practical benefits of this authentication method.	(Thamrongthanakit, T. 2023)
7. Vendor and Supply Chain Cybersecurity Risks	Insufficient vetting of third-party vendors contributes to cybersecurity vulnerabilities, emphasizing the importance of comprehensive supply chain risk management.	(Pandey et al., 2020)
8. Perceived Security vs. Actual Preparedness	Some SMEs may overestimate their cybersecurity resilience, revealing a potential gap between perception and reality that needs addressing.	(Saban et al., 2021)
9. Local Contextualization of Cybersecurity Measures	Importance of tailoring global best practices to the specific challenges and resources available to SMEs in African regions.	(Ahmed et al., 2019; Rawindaran, 2023)

In synthesizing these empirical studies, it becomes evident that the impact of cybersecurity threats on SMEs is a complex interplay of financial, cultural, and contextual factors. The varied findings emphasize the need for a nuanced approach to understanding the specific challenges faced by SMEs in Kajiado County, Kenya. The forthcoming research aims to build upon these global and regional insights to offer a tailored understanding of the cybersecurity landscape for SMEs in the specified locale.

2.4 The Research Gap

The identified research gap in the current literature on the effects of cybersecurity threats on Small and Medium Enterprises (SMEs) in Kajiado County, Kenya, stems from a careful examination of existing studies. While these studies provide valuable insights into various aspects of cybersecurity in SMEs globally and in Kenya, there is a distinct lack of in-depth analysis specific to the unique context of Kajiado County. Several key dimensions contribute to the establishment of this research gap:

Most existing studies focus on global or national perspectives, often overlooking the distinctive characteristics and challenges faced by SMEs in specific regional contexts. The research gap in Kajiado County lies in the absence of a thorough examination of how local factors, such as the economic landscape and regulatory environment, intersect with cybersecurity challenges for SMEs in this specific region.

Empirical analyses within the literature predominantly draw from studies conducted in different regions or countries, neglecting the necessity for localized data. Kajiado County's unique business ecosystem requires dedicated empirical research to capture the region-specific nuances of cybersecurity threats and responses within SMEs.

While there is a wealth of literature on cybersecurity, the focus tends to gravitate towards larger enterprises. The specific challenges faced by SMEs, such as resource limitations, varying levels of digital maturity, and distinct threat landscapes, are often overlooked. This research gap calls for a dedicated exploration of cybersecurity issues tailored to the SME sector in Kajiado County.

The rapid evolution of cyber threats necessitates continuous research to stay ahead of emerging challenges. Many existing studies may lack up-to-date insights into the current threat landscape, potentially overlooking recent developments in cyber-attack tactics. Addressing this gap requires a research approach that considers the dynamic nature of cyber threats.

While some studies provide recommendations for mitigating cybersecurity risks, there is a research gap concerning the effectiveness of these strategies in the local context of Kajiado County. Tailored and comprehensive mitigation strategies that account for the region's specific challenges and resources are yet to be adequately explored in the literature.

In light of these considerations, the research gap in the literature underscores the necessity for an empirical investigation that not only identifies cybersecurity challenges faced by SMEs in Kajiado County but also proposes effective, context-specific solutions. This research aims to bridge this gap by providing a detailed and localized understanding of the cybersecurity landscape for SMEs in this specific region.

3. Research Methodology

3.1. Research Design

This study utilized a comprehensive research design incorporating descriptive, correlational, and comparative methodologies. Specifically, we employed descriptive research to classify the cybersecurity threats that small and medium-sized enterprises (SMEs) in Kajiado County encounter. Our correlational research assessed the immediate and ripple effects of these cybersecurity incidents on these businesses' financial stability and operational efficacy. Furthermore, our comparative research compared factors such as frequency, intensity, current cybersecurity measures, and suggested recommendations among SMEs throughout Kajiado County.

3.2. Data Collection

To ensure comprehensive insights, our data collection approach was multifaceted. Quantitative data on the types of threats, incidents experienced, impacts, and current cybersecurity measures implemented was gathered through surveys and questionnaires distributed among SMEs. For a more in-depth understanding of their experiences and contextual cybersecurity challenges, qualitative data was obtained through interviews and focus groups with SME representatives. In addition, document analysis will be conducted to review any existing records or reports related to cybersecurity incidents within Kajiado County.

3.3. Sampling Strategy

A stratified random sampling technique was employed to ensure representation across different industries and sizes of SMEs. The sample size of 50 SMEs within Kajiado County was determined based on achieving a representative sample for surveys, interviews, and data analysis.

3.4. Data Analysis

Data analysis involved both quantitative and qualitative methods. Quantitative analysis employed statistical tools to analyze survey responses, examining frequencies, and variations in threats, impacts, and cybersecurity measures. Qualitative analysis entailed thematic interviews and focus group data analysis to derive deeper contextual insights.

4. Findings, Analysis, and Discussions

This research provides an in-depth examination of the complex interplay between cybersecurity risks and the functioning of small and medium-sized businesses (SMEs) in Kajiado County, Kenya. It showcases the varied perspectives and experiences that SMEs encounter concerning cybersecurity matters. These include the impact of such threats, the frequency and severity of incidents, the alignment of cybersecurity measures with existing resources, and the efficacy of suggested strategies.

4.1. Types of Cybersecurity Threats

The data study provided insight into how SMEs perceived cybersecurity concerns. Notably, a sizable percentage of respondents (14%) did not consider these dangers to be serious, which may have been caused by a lack of knowledge or strong security measures already in place. Although they may be aware of the dangers, the 24% of respondents who gave the severity a level 2 may not have noticed any major effects.

This may indicate that they have implemented strong cybersecurity safeguards or that they are underestimating the seriousness of these risks. To gain a deeper understanding of the motivations underlying these perceptions, more research might be helpful. Investigating the respondents' degree of cybersecurity expertise, the safeguards they have put in place, and their prior encounters with cybersecurity risks could all be part of this.

Three-quarters of the respondents (18) thought that cybersecurity dangers were moderately serious. This suggested a sober grasp of the possible dangers and repercussions connected to cybersecurity concerns. Furthermore, level 4 was assigned by ten (20%) of the respondents to the seriousness of cybersecurity concerns. These respondents may have witnessed or experienced major effects, and they were likely aware of the grave consequences of cybersecurity risks. Of the respondents, only three (6%) thought that cybersecurity dangers were extremely serious. These individuals may have personally suffered significant consequences as a result of cybersecurity risks, or they may have been well aware of the possible harm these attacks could bring.

The distribution of responses throughout the scale indicates that SMEs have differing opinions about how serious cybersecurity concerns are. Different knowledge levels, experiences with cybersecurity crises, and the strength of current cybersecurity procedures are a few possible reasons for this variation. To guarantee that all SMEs were aware of and capable of fending off possible cybersecurity threats, it emphasized the significance of ongoing education and strong cybersecurity strategies.

4.2. Impact of Cybersecurity Incidents

4.2.1. Operational Inefficiencies

On the impact of cybersecurity incidents on operational efficiencies. The responses indicate a wide range of experiences, from those who have not been significantly affected by cybersecurity incidents (10% strongly disagreed) to those who have experienced significant operational disruptions due to such incidents (14% strongly agreed). This diversity in responses could be due to a variety of factors, including the strength of the security measures in place, the nature of the cybersecurity incidents encountered, and the resilience of the operations to disruptions. It would be interesting to delve deeper into the data to understand the specific circumstances and factors that led to these responses.

4.2.2. Financial Stability

In the survey, 8% of respondents strongly disagreed that cybersecurity incidents impacted their financial stability, potentially attributing this to having robust financial buffers or insurance. Additionally, 18% expressed disagreement, suggesting only minor financial impacts were experienced. A further 22% remained neutral, indicating the presence of some financial impacts but not to a significant extent. On the other hand, 34% agreed that they indeed experienced notable financial impacts due to cybersecurity incidents. Lastly, 18% strongly agreed, signifying that they faced significant financial repercussions. This retrospective data emphasizes the critical link between robust cybersecurity measures and financial safeguards.

It also brings to light the diverse degrees of preparedness and resilience observed among different entities, showcasing the need for tailored approaches in addressing cybersecurity challenges. The spread of responses across the scale suggested a diversity of perceptions regarding the impact of cybersecurity incidents among SMEs. This diversity could have been attributed to various factors such as differences in experiences with cybersecurity incidents, financial resilience, and operational robustness. It underscored the importance of robust cybersecurity strategies to mitigate potential impacts on both operational efficiencies and financial stability.

4.3. Frequency and Intensity of Cybersecurity Threats

Cybersecurity dangers were deemed extremely rare by 6% of respondents. This number might indicate that these organizations either had strong security policies in place or had not faced any serious threats. A further 11% of participants said that dangers were rare, suggesting that they may have run with small-scale threats throughout their activities.15% of respondents expressed no opinion, indicating that while they may have encountered occasional cybersecurity concerns, this was not the case frequently.

As a result, 12% of respondents said the dangers were frequent, suggesting that they had probably encountered significant cybersecurity problems before. Furthermore, 6% of respondents said the threats were extremely regular, suggesting that they had probably come across serious threats frequently.

4.3.1. Intensity of Cybersecurity Threats

In assessing the intensity of cybersecurity threats, a notable 5% of respondents perceived the threats as very in Cybersecurity dangers were deemed extremely rare by 6% of respondents. This number might indicate that these organizations either had strong security policies in place or had not faced any serious threats. A further 11% of participants said that dangers were rare, suggesting that they may have run with small-scale threats throughout their activities.15% of respondents expressed no opinion, indicating that while they may have encountered occasional cybersecurity concerns, this was not the case frequently.

As a result, 12% of respondents said the dangers were frequent, suggesting that they had probably encountered significant cybersecurity problems before. Furthermore, 6% of respondents said the threats were extremely regular, suggesting that they had probably come across serious threats frequently.

Frequent, possibly suggesting the presence of robust security measures effectively mitigating such occurrences. Another 17% of respondents viewed the intensity as infrequent, hinting at the likelihood of experiencing minor threats. A larger portion, constituting 24% of respondents, remained neutral in their perception, suggesting that they might have encountered some threats, but not of high intensity.

On the contrary, 25% of respondents perceived the intensity as frequent, indicating a likelihood of experiencing notable threats. Additionally, 13% of respondents perceived the intensity as very frequent, pointing to a significant 8% who likely encountered high-intensity threats. This data underscores the varied degrees of threat intensity perceived by different respondents, highlighting the need for a nuanced understanding and tailored cybersecurity strategies.

The spread of responses across the scale suggested a diversity of perceptions regarding the frequency and intensity of cybersecurity threats among SMEs. This diversity could have been attributed to various factors such as differences in experiences with cybersecurity threats, the effectiveness of their cybersecurity measures, and their exposure to different types of threats. It underscored the importance of robust cybersecurity strategies to mitigate potential threats and their impacts.

4.4. Cybersecurity Measures - Alignment with Available Resources

The data provided indicated the perceptions of respondents regarding the alignment of cybersecurity measures with available resources within SMEs. From the analysis it was evident that the majority of respondents (16 out of 50) felt that the alignment was moderate, indicating a somewhat balanced integration of cybersecurity measures with the resources available. This suggested that while some cybersecurity measures were in place and functioning adequately, there may have been room for improvement.

A significant number of respondents (20 out of 50) rated the alignment as 2 or "Not well at all," suggesting that they perceived a lack of adequate alignment between cybersecurity measures and available resources. This could have indicated potential gaps in cybersecurity practices, possibly due to resource constraints or a lack of understanding of effective cybersecurity strategies.

On the other hand, a smaller group of respondents (14 out of 50) rated the alignment as 4 or "Extremely well." This suggested that some SMEs successfully aligned their cybersecurity measures with their available resources, possibly due to effective cybersecurity strategies and sufficient resource allocation. These diverse perceptions highlighted the varying degrees of alignment or misalignment of cybersecurity measures with available resources within SMEs. It underscored the need for tailored strategies that considered the specific resources of each SME to enhance cybersecurity effectively.

4.5. Recommendations and Strategies - Effectiveness of Proposed Strategies

Respondents' perceptions regarding the effectiveness of proposed cybersecurity strategies within SMEs, the research noted that most respondents (14 out of 50) found the proposed strategies to be moderately effective. This suggested that while the strategies were somewhat effective, there might have been room for improvement or a need for more tailored approaches.

A significant number of respondents (19 out of 50) rated the effectiveness as 2 or "Not effective at all". This indicated a perception that the proposed strategies were not sufficiently effective, possibly due to a lack of relevance to the specific cybersecurity challenges faced by the SMEs or a lack of resources to implement the strategies effectively.

Conversely, a smaller group of respondents (17 out of 50) rated the effectiveness as 4 or "Extremely effective". This suggested that some SMEs found the proposed strategies highly effective, possibly due to a good fit with their specific cybersecurity needs and available resources. These mixed perceptions highlighted the varying degrees of effectiveness of the proposed cybersecurity strategies within SMEs. It underscored the need for strategies that were adaptable and tailored to the specific needs and resources of each SME to enhance cybersecurity effectively.

4.6. Descriptive statistics

For descriptive statistics, the mean value of 2.74 suggests that SMEs perceive these threats to be moderately severe. However, the standard deviation indicates a significant variability in these perceptions. The study also found that SMEs perceive a moderate impact on operational inefficiencies, with a mean value of 3.16. When it comes to financial stability, the perceived impact is slightly higher, with a mean value of 3.32. Again, the standard deviation points to a variability in these perceptions.

On the frequency and intensity of cybersecurity threats, SMEs perceive these threats to occur at a moderate frequency, with a mean value of 2.9. The perceived intensity of these threats is also moderate, with a mean value of 3. The standard deviation in both cases indicates a variability in these perceptions. On average, SMEs perceive a moderate alignment, with a mean value of 2.76. The standard deviation suggests a variability in these perceptions. The effectiveness of proposed strategies is perceived to be moderately effective, with a mean value of 2.94. The standard deviation indicates a variability in these perceptions.

The descriptive statistics provide insights into the central tendency and variability of perceptions among SMEs regarding various aspects of cybersecurity. Across all sections, the mean values indicate moderate perceptions among SMEs regarding cybersecurity threats, the impact of incidents, frequency, and intensity of threats, alignment of measures with resources, and effectiveness of proposed strategies. The standard deviations highlight the variability in responses, indicating that while there are moderate average perceptions, there is also diversity in individual perceptions among SMEs.

5. Cybersecurity Perceptions and Experiences among SMEs in Kajiado County

The survey results revealed a wide range of perceptions and experiences among SMEs about cybersecurity threats. The SMEs encountered various cybersecurity threats, indicating the pervasive nature of these risks in the digital landscape. The diversity of threats underscored the need for comprehensive cybersecurity measures that could address a broad spectrum of potential risks.

The impact of these threats on SMEs varied, reflecting the differing levels of preparedness and resilience among these businesses. Some SMEs had robust cybersecurity measures in place that mitigated the impact, while others were more vulnerable due to limited resources or a lack of awareness. The frequency and intensity of cybersecurity incidents experienced by SMEs further highlighted the persistent and evolving nature of these threats. This called for continuous monitoring and updating of cybersecurity measures to keep pace with emerging threats.

The alignment of cybersecurity measures with available resources was a critical factor in the effectiveness of these strategies. SMEs with limited resources may have struggled to implement comprehensive measures, emphasizing the need for cost-effective and scalable solutions. The mixed perceptions regarding the effectiveness of the proposed strategies suggested that a one-size-fits-all approach may not have been suitable. The varying needs and resources of SMEs necessitated tailored strategies that considered the specific context of each business.

6. Research Recommendations

6.1. Cybersecurity Awareness and Training

Prioritize cybersecurity awareness and training programs for all employees in SMEs. Given the varied levels of digital literacy in Kenya, training should cover basic cybersecurity hygiene practices, such as identifying phishing attempts, the importance of regular password updates, and securing personal devices used for work. Cultivating a culture of cybersecurity mindfulness can significantly reduce the risk of breaches.

6.2. Utilize Free or Low-Cost Security Tools

Leverage free or cost-effective cybersecurity tools specifically designed for SMEs. This can include antivirus software, firewall technologies, and secure communication platforms. Recommendations should include guidance on resources available for SMEs, possibly through government or non-profit initiatives aimed at bolstering national cybersecurity resilience.

6.3. Data Protection Strategies

Implement data protection strategies adapted to the scale of SME operations. This can involve simple, yet effective measures like regular data backups, encryption of sensitive information, and access controls to protect against unauthorized access. Tailoring these strategies to the specific type of data handled by an SME can enhance their effectiveness.

6.4. Incident Response Planning

Develop and formalize an incident response plan. Despite having limited resources, SMEs can benefit significantly from having a clear plan in case of a cybersecurity incident. This plan should include steps to contain the breach, assess and mitigate damages, and communicate with stakeholders, along with a post-incident review process to prevent future occurrences.

6.5. Collaboration and Sharing of Cybersecurity Intelligence

Encourage collaboration among SMEs in Kajiado County through sharing platforms or consortiums for cybersecurity intelligence. By sharing insights on threats and effective defense mechanisms, SMEs can collectively enhance their cybersecurity posture. This could be facilitated through local business associations or chambers of commerce.

6.6. Customized Cybersecurity Consultancy Services

Promote the development and use of customized cybersecurity consultancy services that understand the local business environment and can offer practical, cost-effective solutions for SMEs. These services could range from initial vulnerability assessments to ongoing cybersecurity management support.

Contextualizing global cybersecurity best practices within the regional specifics of Kajiado County, Kenya, SMEs can develop a robust defense against cyber threats, ensuring their performance and sustainability in the digital age.

Questionnaires Instruments

Dear Participant,

Greetings! We appreciate your participation in this important research study, which aims to delve into the multifaceted landscape of cybersecurity threats and their potential impact on the performance of Small and Medium Enterprises (SMEs). This research focuses specifically on SMEs within the unique context of Kajiado County, Kenya.

Title: Exploring the Impact of Cybersecurity Threats on Small and Medium Enterprises' Performance: A Case Study of Kajiado County, Kenya.

As technology continues to play an increasingly integral role in business operations, the significance of cybersecurity cannot be overstated. Small and Medium Enterprises, being the backbone of many economies, are particularly vulnerable to the ever-evolving landscape of cyber threats. Understanding the nature, severity, and consequences of these threats is crucial for developing effective strategies to safeguard businesses and sustain their growth.

This research seeks to investigate the experiences of SMEs in Kajiado County with cybersecurity threats over the past year. We aim to gain insights into the severity, frequency, and intensity of these threats, as well as their potential impact on operational efficiency, financial stability, and overall business performance.

Your valuable input as a participant in this study will contribute significantly to advancing our understanding of the challenges faced by SMEs in Kajiado County in the realm of cybersecurity. The findings of this research will not only provide a comprehensive overview of the current cybersecurity landscape but also inform policymakers, business owners, and cybersecurity professionals about the specific needs and vulnerabilities of SMEs in the region.

Rest assured that your responses will remain confidential, and the data collected will be used solely for research purposes. Your time and insights are immensely valuable, and we thank you in advance for your cooperation.

If you have any questions or concerns regarding the questionnaire or the research study, please feel free to contact [Researcher's Name] at [Contact Information].

Thank you for being a vital part of this endeavor.

Sincerely,

[Your Name] : ………………………………………………………………

[Your Title] : ………………………………………………………………

[Institution or Organization] : ………………………………………………………………

Section 1: Types of Cybersecurity Threats

1. What types of cybersecurity threats has your business encountered in the past year? (Options: Malware, Phishing, Man-in-the-middle attack, Denial-of-service attack, SQL injection, Zero-day exploit, DNS Tunneling, etc.):

   ………………………………………………………………………………

2. How would you categorize the severity of these threats? (Options: Low, Medium, High)

   : …………………………………………

Section 2: Impact of Cybersecurity Incidents

3. Have you noticed any operational inefficiencies as a result of cybersecurity incidents? (Options: Yes, No)
4. : ………………………………………….
5. If yes, can you estimate the percentage decrease in operational efficiency?
6. : ………………………………………….
7. Have cybersecurity incidents impacted your business's financial stability? (Options: Yes, No)
8. : …………………………………………….
9. If yes, can you estimate the percentage of financial loss?

   : …………………………………..

Section 3: Frequency and Intensity of Cybersecurity Threats

10. How often do you encounter cybersecurity threats? (Options: Daily, Weekly, Monthly, Yearly)

    : …………………………………

doi:10.20944/preprints202411.0237.v1

11. On a scale of 1-10, how would you rate the intensity of the cybersecurity threats your business faces?

    : ……………………………………

Section 4: Cybersecurity Measures

12. What cybersecurity measures has your business implemented? (Open-ended)

    :

    ……

    ……

    ………………………………………………………………………………………..

13. How do these measures align with your available resources? (Options: Aligns well, partially aligns, does not align)

    : …………………………………………………………

Section 5: Recommendations and Strategies

14. What strategies would you recommend for dealing with cybersecurity threats in Kajiado County? (Open-ended):

    ……

    ……

    ………………………………………………………………………………………………

15. How effective do you think these strategies would be in addressing the specific challenges faced by SMEs in Kajiado County? (Options: Very effective, somewhat effective, Not effective)

    : ………………………………………………

16. **Likert scale questions for the questionnaire:**

Section 1: Types of Cybersecurity Threats	**1 = Not severe at all**	**2**	**3**	**4**	**5 = Extremely severe**

Severity of cybersecurity threats					

Section 2: Impact of Cybersecurity Incidents	**1 = Strongly disagree**	**2**	**3**	**4**	**5 = Strongly agree**
Operational inefficiencies					
Financial stability					

Section 3: Frequency and Intensity of Cybersecurity Threats	**1 = Very infrequent**	**2**	**3**	**4**	**5 = Very frequent**
Frequency of cybersecurity threats					
Intensity of cybersecurity threats					

Section 4: Cybersecurity Measures	**1 = Not well at all**	**2**	**3**	**4**	**5 = Extremely well**
Alignment with available resources					

Section 5: Recommendations and Strategies	**1 = Not effective at all**	**2**	**3**	**4**	**5 = Extremely effective**
Effectiveness of proposed strategies					

References

Amoit Enaga, L., & Naomi Kathula, D. (2022). The Adoption of Technology to an Enhanced SME Growth; A Survey of SMES In Amukura Town, Busia County. In *African Journal of Emerging Issues (AJOEI). Online ISSN* (Vol. 7, Issue 4).

Barasa, L., & Kiiru, J. M. (2023). The Digital Economy and Youth Employment in Africa. In *Public Policy and Technological Transformations in Africa* (pp. 161–182). Springer International Publishing. https://doi.org/10.1007/978-3-031-18704-9_7

Borah, S., Kama, C., Rakshit, S., & Vajjhala, N. R. (2022). *Applications of Artificial Intelligence in Small- and Medium-Sized Enterprises (SMEs)* (pp. 717–726). https://doi.org/10.1007/978-98116-8763-1_59

Chege, S. M., & Wang, D. (2020). The influence of technology innovation on SME performance through environmental sustainability practices in Kenya. *Technology in Society*, *60*, 101210. https://doi.org/10.1016/j.techsoc.2019.101210

Hamed Taherdoost. (2022). An Overview of Trends in Information Systems: Emerging Technologies that Transform the Information Technology Industry. *Cloud Computing and Data Science*, *23*(2), 1–16. https://doi.org/10.37256/ccds.4120231653

Henderson, D. (2023). Boundary work in the regional innovation policy mix: SME digital technology diffusion policies in Wales. *Science and Public Policy*, *50*(3), 548–558. https://doi.org/10.1093/scipol/scad006

Kiboi, B. N. (2015). *CYBER SECURITY AS AN EMERGING THREAT TO KENYA'S NATIONAL SECURITY*.

Leonard, C., Ogara, S., Wakoli, W., & Liyala, S. (2020). *An Understanding of The Cyber Security Threats And Vulnerabilities Landscape: A Case of Banks in Kenya*. www.ijiras.com|

Mantha, B., García de Soto, B., & Karri, R. (2021). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society*, *82*(66), 10–26. https://doi.org/10.1016/j.scs.2020.102682

Morgante, E., & Fabian Wallace-Stephens. (2021).

pathfinding_the_future_of_work_in_sub_saharan_africa.

Mwangi, B. J., & Brown, I. (2015). A Decision Model of Kenyan SMEs' Consumer Choice Behavior in Relation to Registration for a Mobile Banking Service: A Contextual Perspective. *Information Technology for Development*, *21*(2), 229–252. https://doi.org/10.1080/02681102.2013.874320

Mwania Kasyuma. (2016). *Cyber Threats and Cyber Security in ISO Certified Organizations in Kenya*.

Ngetich, B., & Migosi, J. (2023). Management Practices and Sustainability of Training Programs: A Case of Digital Skills Training Projects in Kibera Slums, Nairobi City County, Kenya. *IRA International Journal of Management & Social Sciences (ISSN 2455-2267)*, *19*(3), 45. https://doi.org/10.21013/jmss.v19.n3.p1

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity Strategy's Role in Raising Kenyan Awareness of Mobile Internet Threats. *Information & Security: An International Journal*, *32*, 155–174. https://doi.org/10.11610/isij.3207

Pawar, S., & Palivela, Dr. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Sambuli, N., Maina, J., & Kamau Tyrus. (2016). *Mapping the Cyber Policy Landscape: Kenya*. https://www.flickr.com/photos/ndave/

Sutherland, E. (2018). Digital Privacy in Africa: Cybersecurity, Data Protection &amp; Surveillance.
SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3201310

Thompson, J. (2023). *Factors Influencing Cybersecurity Risk Among Minority-Owned Small Businesses* (Vol. 6, Issue 1).

Victor Chitechi, K., Mbugua, S., & Omieno, K. (2018). Facilitating Factors for Cybersecurity Vulnerabilities in Kenyan County Governments. *Asian Journal of Research in Computer Science*, 1–11. https://doi.org/10.9734/ajrcos/2018/v2i124773

Ikovo, V. N. (2018). University Of Nairobi College of Biological and Physical Sciences School Of
Computing and Informatics Cyber Security Preparedness Assessment Toolkit.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.