

**UNIVERSITY OF NAIROBI**  
**FACULTY OF ARTS AND SOCIAL SCIENCES**  
**DEPARTMENT OF SOCIOLOGY, SOCIAL WORK & AFRICAN WOMEN**  
**STUDIES**

**THE EFFECTS OF CYBERCRIME ON PERFORMANCE OF SMALL AND**  
**MEDIUM ENTERPRISES (SMEs) IN NAIROBI COUNTY, KENYA**


**Jacinta Nduku Mulei (C50/33065/2019)**

**A Project Paper submitted in the partial fulfillment of the requirements for the**  
**Award of Master of Arts in Criminology and Social Order.**

**November 2023**

## DECLARATION

This project paper is my original work, and it has never been submitted to any institution for credit in academic.

Signed:  \_\_\_\_\_ Date: 2<sup>nd</sup> November 2023 \_\_\_\_\_

Student: **Jacinta Nduku Mulei (C50/33065/2019)**

Email address: **Muleijacinta@students.uonbi.ac.ke**

This project paper has been submitted for examination with my approval as university supervisor.

Signed:  \_\_\_\_\_ Date: 6<sup>th</sup> November 2023 \_\_\_\_\_

**Prof. Edward Ontita**

Department of Sociology, Social Work & African Women Studies

University of Nairobi

**DEDICATED**

This work is dedicated to fraud risk management officers entrusted with the responsibility of fighting fraud within organizations.

## **ACKNOWLEDGEMENT**

I would like to recognize the indispensable support, guidance and encouragement given by my supervisor, Prof. Ontita and my family during the project writing.

## TABLE OF CONTENTS

<b>DECLARATION.....</b>	<b>ii</b>
<b>DECLARATION.....</b>	<b>iii</b>
<b>ACKNOWLEDGEMENT.....</b>	<b>iv</b>
<b>TABLE OF CONTENTS .....</b>	<b>v</b>
<b>LIST OF TABLES .....</b>	<b>viii</b>
<b>LIST OF FIGURES .....</b>	<b>ix</b>
<b>ABBREVIATIONS.....</b>	<b>x</b>
<b>ABSTRACT.....</b>	<b>xi</b>
<b>CHAPTER ONE: INTRODUCTION.....</b>	<b>1</b>
1.1 Background of the Study.....	1
1.2 Statement of the Problem .....	3
1.3 Research Gap.....	5
1.4 Research Questions .....	6
1.5 Purpose of the study .....	6
1.6 Objectives of the Study .....	6
1.7 Value of the Study.....	7
1.8 Scope of the study .....	8
<b>CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FRAMEWORK.....</b>	<b>9</b>
2.1 Introduction .....	9
2.2.1 Data Breach and Performance .....	9
2.2.2 Identity Theft and Performance.....	11
2.2.3 Phishing and Performance .....	14
2.2.4 Malware Attacks and Performance.....	16
2.2.5 Role of Kenyan Government in Cyber Security.....	18
2.3 Theoretical Framework .....	20
2.5 Conceptual Framework .....	21
<b>CHAPTER THREE: RESEARCH METHODOLOGY .....</b>	<b>23</b>
3.1 Introduction .....	23
3.2 Research Design.....	23

3.3 Target Population .....	23
3.4 Sample Design.....	25
3.5 Data Collection Methods.....	26
3.5.1 Surveys .....	26
3.5.2 Key Informant Interviews.....	26
3.5.3 Observations .....	27
3.5.4 Desk Review.....	27
3.6 Data Collection Tools.....	27
3.6.1 Questionnaire.....	27
3.6.2 Key Informant Interview Guide .....	28
3.6.3 Secondary Sources of Data.....	28
3.7 Pilot Study .....	28
3.7.1 Validity of the Research Instruments .....	28
3.7.2 Reliability of the Research Instruments.....	29
3.8 Data Analysis .....	29
3.8.1 Quantitative Data Analysis.....	29
3.8.2 Qualitative Data Analysis.....	30
3.9 Ethical Considerations.....	31
<b>CHAPTER FOUR: DATA ANALYSIS AND PRESENTATION.....</b>	<b>32</b>
4.1 Introduction .....	32
4.2 Demographic Information .....	32
4.2.1 Demographic Information of the SME owners .....	32
4.3 Profiles of the SMESs .....	35
4.4 Descriptive Analysis .....	36
4.4.1 Data Breach .....	36
4.4.2 Identity Theft .....	47
4.4.3 Phishing .....	55
4.4.4 Malware Attack .....	61
4.5 Performance of the SMEs .....	69
4.6 Regression Analysis .....	72
<b>CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.</b>	<b>76</b>

5.1 Introduction .....	76
5.2 Summary of the Findings .....	76
5.3 Conclusions .....	78
5.4 Recommendations of the Study.....	79
5.5 Suggestions for Further Studies .....	80
<b>REFERENCES.....</b>	<b>81</b>
<b>APPENDICES .....</b>	<b>87</b>
<b>APPENDIX I: QUESTIONNAIRE FOR SME’S BUSINESS OWNERS .....</b>	<b>87</b>
<b>APPENDIX II: KEY INFORMANT INTERVIEW GUIDE.....</b>	<b>96</b>

## LIST OF TABLES

Table 4. 1: Gender.....	32
Table 4. 2: Age of SME owners.....	33
Table 4. 3: Level of Education.....	34
Table 4. 4: Time in Operation.....	35
Table 4. 5: Frequency of Using Technology Devices.....	36
Table 4. 6: Type of Information Recorded on the Databases .....	38
Table 4. 7 Access to the SME Database .....	40
Table 4. 8: Type of Information Stolen from the SME Database.....	44
Table 4. 9: Personnel with Access to the SME Contact List .....	48
Table 4. 10: Change of Passwords on SME Electronic Devices .....	51
Table 4. 11: Personnel Responsible for Conducting Updates on SMEs’ Electronic Devices.....	62
Table 4. 12: Frequency of Updating Anti-virus Applications .....	64
Table 4. 13: Financial Performance of SMEs (2017-2021).....	70
Table 4. 14: Non –Financial Performance .....	71
Table 4. 15: Model Summary .....	73
Table 4. 16: ANOVA.....	73
Table 4. 17: Coefficient of Determination.....	74



## LIST OF FIGURES

Figure 1. 1: Conceptual Framework .....	22
Figure 4. 1: SME's Database .....	37
Figure 4. 2: Occurrence of Data Breach .....	42
Figure 4. 3: Copying Data from the SME Computer to Personal IT Devices .....	49
Figure 4. 4: Passwords on SME Electronic Devices.....	50
Figure 4. 5: Verification of Electronic and Plastic Payments.....	52
Figure 4. 6: Victims of Identity Theft.....	53
Figure 4. 7: Clicking of Pop-ups of SMEs' Computers.....	55
Figure 4. 8: Confirmation of Invoices Before Making Payments.....	57
Figure 4. 9: Opening Emails form Trusted Individuals and Businesses Only .....	58
Figure 4. 10: Emails Soliciting SMEs Confidential Information .....	59
Figure 4. 11: Anti-Virus Application.....	63
Figure 4. 12: Media Download .....	65
Figure 4. 13: Data Back-up.....	66
Figure 4. 14: Computer Crush due to Malware Attack.....	67

## ABBREVIATIONS

<b>AV:</b>	Antivirus
<b>BYOD:</b>	Bring Your Device
<b>CBD:</b>	Central Business District
<b>DBA:</b>	Data Breach Announcement
<b>GDP:</b>	Global Domestic Product
<b>IITRC:</b>	Internal Identity Theft-Related Crimes
<b>IT:</b>	Information Technology
<b>IITRC:</b>	Identity Theft Resource Center
<b>ITS:</b>	Identity Theft Supplement
<b>KIPPRA:</b>	Kenya Institute for Public Policy Research and Analysis
<b>MSME:</b>	Micro, Small, and Medium Enterprises
<b>NCVS:</b>	National Crime Victimization Survey
<b>NGOs:</b>	Non-Governmental Organizations
<b>PRC:</b>	Privacy Rights Clearinghouse
<b>RAT:</b>	Routine Active Theory
<b>ROA:</b>	Return on Asset
<b>ROE:</b>	Return on Equity
<b>SEM:</b>	Structural Equation Modeling
<b>SME:</b>	Small and Medium Enterprises
<b>UK:</b>	United Kingdom

## **ABSTRACT**

Small and Medium Enterprises (SMEs) are the backbone of Kenya's economy. However, due to their nature of business operations SMEs typically lower their costs on information technology to the extent that they outsource any digital services, occasionally encourage employees to use Bring Your Device (BYOD) and depend on cloud services at work as a strategy to save finances on technology devices. This makes the SMEs susceptible to cybercrime. The purpose of this study was to investigate the influence of cybercrime on the operational performance of Nairobi-based SMEs. The specific objectives included determining the impact of data breaches, identity theft, phishing, and malware attacks on the performance of SMEs. The study used a cross-sectional descriptive research approach, focusing on SME owners in Nairobi County's Kamukunji constituency. The study used a simple random sampling approach to choose 358 SMEs in the Kamukunji constituency as its sample population. Data was collected via questionnaires, a key informant interview guide, and secondary sources, and it included both quantitative and qualitative features. Quantitative data was evaluated and displayed in tables and figures using descriptive and inferential statistics. Meanwhile, qualitative data gathered through interviews and open-ended questions was analyzed and presented in narrative form. Cronbach's Alpha dependability was used to determine the instruments' reliability. The study's findings revealed that cybercrime has a negative influence on the performance of SMEs. Specifically, the findings indicate that data breaches had a significant impact on consumer behavior, which in turn affected the success of SMEs. The study also revealed that data breaches occurred due to the easy access of SME information on social media platforms. This had resulted in more businesses being vigilant of the customers making electronic payments. Further, the findings revealed that phishing and malware attacks were a problem faced by SMEs who had not invested in establishing effective cyber security strategies. In this regard, the study recommends that SMEs should work hand in hand with ICT specialists/experts to ensure that their business information is secure and protected. This provides a good working environment since the focus of the SMEs will be in generating income, hence improving performance.

## **CHAPTER ONE: INTRODUCTION**

### **1.1 Background of the Study**

Businesses have access to information technology, which offers opportunities for social and economic advancement. Businesses' ability to create, commercialize and reap economic advantages through adoption of technology and innovations is crucial for improving performance (Ekaterina, 2010). This has caused the corporate environment to change as a result of faster and more effective ways to conduct business as a result of technology, economic pressures, and competition. With the onset of global competition and the widespread adoption of technology sharing information between countries has become easy (Wekunda, 2015). With many people relying on the internet, security concerns have risen to the top of people's minds when it comes to global well-being. Cybercrime is one of the most serious issues that technology users face (Nfuka, Sanga, and Mshangi, 2015).

Cybercrime is a broad phrase that encompasses any illicit activities carried out through the use of computers, the internet, the global web, and cyberspace (Nkurunziza, 2021). Any criminal conduct involving computers and networks is classified as cybercrime. Cybercrime is measured using data breaches, identity theft, phishing, and malware attacks. Data breaches occur when unauthorized access to a computer network or device results in the theft or exposure of sensitive information, such as personal or financial data (Janakiraman, Lim, & Rishika, 2018). Identity theft occurs when an individual's personal details, such as their name, address, social security number, or credit card information, are unlawfully obtained for the purpose of perpetrating fraud or engaging in other illegal activities (Rakololo & Malule, 2018). Phishing is the act of sending misleading emails,

messages, or websites that pretend to be from credible sources in order to trick people into disclosing personal information or unknowingly installing malware (Iuga, Nurse, & Erola, 2016). Malware assaults involve entering a computer system with malicious software intended to do harm, such as data theft, file damage, or system seizing (Silva, 2020). Cybercrime has been on the rise across the globe. Warner (2011) identified that the shortcoming witnessed by security organizations to put in place effective legal frameworks to deal with cyber criminals is a driver for cybercrime. The absence of a unified and cohesive legal framework for the enforcement of cybercrime is a result of varying perspectives on how to prosecute cyber criminals (Brenner & Koops, 2004).

Firm performance is defined as a company's actual output or yield compared to its expected outcomes or objectives. Triandis (2015) divides "firm performance" into three components: shareholder return, product-market performance, and financial performance. The assessment of firm performance involves the use of accounting-based financial indicators and market-based indicators, as outlined by Ongore et al. (2008). This is with the realization that overreliance of financial indicators may provide biased findings. Therefore, to clearly understand the performance of SMEs, both financial and non-financial measures were assessed.

Small and medium enterprises (SMEs) are the backbone of Kenya's social and economic development and a decline in GDP results to unemployment and economic hardships by the families. SMEs play an important role in Nairobi, accounting for around 20% of the city's GDP. Furthermore, this industry is a key employer, employing more than 85% of the city's workforce. Over 2 million people rely on the operations and activities of SMEs in Nairobi for a living (Government of Kenya-GOK, 2018). However, because of their

business style, the majority of SMEs are victims of cybercrime. SMEs typically reduce information technology costs to the point where the company outsources technology services; SMEs rely heavily on cloud services, and some employees are forced to use BYOD (Bring Your Device) at work to save money on technology equipment, which exposes them to viruses and worms at their workplaces. According to Wekunda (2015), SMEs are victims of cybercrime because most of them have ties to large corporations or organizations, and hence are utilized as a conduit to target larger corporations. Twisdale (2018) expands on SMEs, claiming that due to their cost-cutting attitude, they are more likely to be victims of denial-of-service attacks in instances where they have been hacked or pay a high price to recover from attacks since a majority lack contingency plans in place. As a result, failing to put in place procedures to combat cybercrime may result in the Kenyan economy contracting leading to unemployment, inequality and poverty.

## **1.2 Statement of the Problem**

Technology's exponential expansion, increased capacity, accessibility, and lower cost have resulted in revolutionary advances in business, communications, entertainment, and education. But as capability rises, so does vulnerability. Information technology has started to give 'thieves' opportunities they could never have dreamed in the past (Mwai, 2015). Both the number of possible casualties and the number of prospective perpetrators of computer-related crime have expanded due to the increasing rate at which gadgets may connect to share information. However, due to the intricacy of such crimes and the evasive nature of cyber thieves, detecting and preventing them has become increasingly challenging. Computer crimes have rapidly expanded in recent years, outpacing the government's and other sectors' ability to adequately protect their networks.

SMEs are the backbone of Kenya's economy. Because of their business approach, the majority of SMEs are victims of cybercrime (Wekunda, 2015). Due to their nature of business operations SMEs typically lower their costs on information technology to the extent that they outsource any digital services, occasionally encourage employees to use Bring Your Device (BYOD) and depend on cloud services at work as a strategy to save finances on technology devices. According to Wekunda (2015), SMEs are victims of cybercrime because most of them have ties to large corporations or organizations, and hence are utilized as a conduit to target larger corporations. Nkurunziza (2021) elaborates on SMEs, claiming that due to their cost-cutting attitude, they are more likely to fall prey to denial-of-service assaults, where their server may be hacked, or pay a high price for recovery since most of these businesses do not have contingency plans in place. Due to their limited resources, SMEs are prone to software piracy, trade and logo attacks, and may be unable to detect unauthorized use of their trademarks on the internet.

Globally, studies such as Twisdale (2018) assessed SME vulnerabilities to cyber-criminal activities in the USA and established that SMEs are vulnerable to cybercrime since they do not consider cyber security a necessity. Further, Kumar, Ojha, and Srivastava, (2018) in India, found that in SMEs, the current anti-malware security is insufficient due to lack of resources. The authors observed that SMEs fail to invest in cyber security due to its high cost. Rakololo and Maluleke (2020) looked at the factors driving identity theft in South Africa. The findings show that having an understanding of identity document (ID) theft can help address cybercrime since the nature of the crime is identified. While the study revealed the extent to which identity theft has increased over the years, the study did not show its influence on firm performance, a gap that the current study intends to address.

However, these studies did not specifically address SMEs in Kenya. Moreover, the studies evaluated cybercrimes within the SME sector and failed to show their influence on performance.

In Kenya, Chesimo's (2020) study looked into the elements that promote fraudulent transactions and their impact on non-governmental organizations (NGOs') operational effectiveness in Nairobi County. The study found that cyber security was critical for the survival of NGOs. A study by Silva, (2020) investigated malware attacks on organizations. The study used secondary data for analysis. The absence of reliable frequency monitoring and the effects of these types of cyber-attacks, according to the report, make it difficult for the healthcare industry to properly safeguard its networks. The study however, though based in Kenya, was not specific to SME, an essential sector to the Kenyan economy. This study aimed at showing the effect of cybercrime (measured by data breach, identity theft, phishing and malware attacks) and performance. Therefore, this study sought to determine the effect of cybercrime on performance of SMEs in Kenya by answering the research question, what is the effect of cybercrime on performance of SMEs in Kenya?

### **1.3 Research Gap**

The rate of cybercrime within the context of business operations has increased in the 21<sup>st</sup> Century as a result of technological advancements. The rise in cybercrime in SMEs is attributed to the fact that most of these SMEs as elaborated by Nkurunziza (2021) do not invest in cyber security unlike large corporations as indicated by the Routine Active theory. This realization has driven scholars to conduct different studies to show the effect of cybercrime on performance. However, the majority of the studies conducted have focused on developed economies such as Okeke, (2015) in the United Kingdom; Knight (2020) in



the USA; Gadirova, (2021) in the USA. This presents a research gap for further research to be conducted in developing countries such as Kenya. Further, while extant literature showed that cybercrime affects business operations, few studies has been conducted on the performance of SMEs as influenced by cybercrime. This is a gap that this study intended to assess.

#### **1.4 Research Questions**

The study sought to answer the research question: What is the effect of cybercrime on the performance of SMEs within Nairobi County, Kenya?

The specific research questions were:

- i. What is the effect of the data breach on performance of SMEs in Kenya?
- ii. What effect does identity theft have on performance of SMEs in Kenya?
- iii. What is the result of phishing on performance of SMEs in Kenya?
- iv. What is the outcome of malware attacks on performance of SMEs in Kenya?

#### **1.5 Purpose of the study**

The purpose of this study was to determine the effect of cybercrime on performance of SMEs in Kenya.

#### **1.6 Objectives of the Study**

The general objective of the study was to determine effect of cybercrime on performance of SMEs in Nairobi.

The specific objectives of the study were:

- i. To establish the effect of data breach on performance of SMEs in Nairobi County, Kenya.
- ii. To find out the effect of identity theft on performance of SMEs in Nairobi County, Kenya.
- iii. To assess the effect of phishing on performance of SMEs in Nairobi County, Kenya.
- iv. To demonstrate the effect of malware attacks on performance of SMEs in Nairobi County, Kenya.

### **1.7 Value of the Study**

Cybercrimes continue to pose a significant threat to SMEs in the 21<sup>st</sup> Century. Therefore, the findings of this study are helpful to SMEs, as it will give insight into cybercrime within the business sector. The study emphasizes the need for SMEs to engage in cyber security irrespective of their size. Thus, SMEs can use this study to identify cybercrime and implement cyber security measures to continue being competitive.

In addition, the findings will enable the policymakers to put more emphasis on cyber security among all businesses. The policymakers can use the study to formulate strategies and policies that may help in fighting different cybercrimes identified in the study.

The study is also of importance to scholars and academicians. The study can be used by scholars as a point of reference in the field of cybercrime and cyber security. The study also acts as a foundation for further studies to be conducted concerning cybercrime experienced among businesses in the 21<sup>st</sup> Century.

### **1.8 Scope of the study**

The study targeted 5277 SMEs in Kamukunji constituency in Nairobi County. This is because, in the modern world, cybercrime has become an issue of concern in all businesses including SMEs. The study collected data from the owners of the SMEs since they are conversant with the cyber threats they face and the cybercrimes that have occurred in the SMEs. The study data were collected in the month of July 2023. The focus on cybercrime is motivated by the fact that today, technology and globalization have resulted in the emergence of not only more cyber security approaches but also it has led to an increase in cybercriminals.

## **CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FRAMEWORK**

### **2.1 Introduction**

This chapter highlights the literature review, theory anchoring the study and the conceptual framework related to cybercrime and performance of SMEs within Nairobi County, Kenya. It will also discuss the main concepts of cybercrime and theory explaining the motivation behind cybercrime. The critique on existing literature will follow and research gaps shall be expounded.

### **2.2 Literature Review**

#### **2.2.1 Data Breach and Performance**

The effect of a multichannel retailer's data breach announcement (DBA) on consumer behavior was assessed by Janakiraman, Lim, and Rishika (2018). The study relied on empirical data to evaluate the impact DBA has on the spending behaviour of customers and channel movement behaviour by conducting an experiment and using customers' transaction data from the retail stores. The study compared the behavior of a treatment group (consumers whose privacy had been violated) and a control group after the initial DBA using the difference-in-differences modeling framework (customers whose information was not violated). Despite the fact that data breaches cause significant drops in consumer purchasing, the report claims that customers switch from compromised to unhacked channels. The study focused on customer behaviour as influenced by the data breach, this study goes further to look at its effect on the performance of SMEs which by extension is associated with the change in customer behaviour.

A study by Juma'h and Alnsour (2020) looked at the effect data breach has on the success of the company. The authors note that data breaches can have social, legal, and economic consequences. Data were extracted from the Mergent Online database; the data was financial information of the breached companies. Solvency, profitability, and liquidity were used to gauge financial performance. To compare the financial performance of the businesses before and after the data breach, the size of the companies was taken into consideration. According to the survey, organizations that were breached saw a drop in performance during the quarter after the attack. This means that a data breach harms the functioning of a company. The study's biggest flaw is its lack of ratio and trend analysis. When researching accounting data, such analyses are frequently utilized. They do, however, rely on the firm's disclosed financial reports and do not directly reflect the companies' situations and realities. The current research gathered secondary data from the financial statements of Nairobi-based SMEs.

Knight (2020) investigated the data security techniques utilized by small business owners. During the data collection phase of the study, an interview guide was used as the major tool. Four people who had effectively implemented data security techniques were interviewed by the author. The researcher also studied organizational documentation during the data-gathering phase. Two topics emerged from the data analysis: data information assurance and third-party dependency. The study discovered a positive social impact, such as the possibility for small business owners to adopt data security policies to defend their companies from data breaches. Protection from data breaches can help small business owners regain trust and increase expenditure, resulting in improved business success.

Gadirova's study (2021) looked at cyber-attacks that occurred between 2015 and 2019 and their effects on private enterprises' cash holdings. He used the PRC (Privacy Rights Clearinghouse) database to compile data on cybercrime because it provided information on publicly announced attacks. The author also got information from ITRC (Identity Theft Resource Center) yearly reports (for the same years) and a Google search. The purpose of the study was to close this gap by giving empirical proof of the monetary impact of data breaches on private businesses. The author discovered that firms attacked in 2018 boosted their cash holdings significantly, whereas an attack in 2020 can only affect cash holdings while dealing with a firm's tangibility and ROA (Return On Assets). The findings show that data breaches in an organization have a significant influence on performance as measured by ROA. However, the study collected empirical data only. Due to the biased nature of relying on secondary data only, this study also collected primary data to address this challenge.

### **2.2.2 Identity Theft and Performance**

Rakololo and Maluleke (2020) researched the factors that contribute to identity document theft in South Africa. The researcher collected data using two scientific methods: a survey approach (questionnaire) and secondary data gathered through a literature review. A total of 90 people were chosen for this investigation on a quantitative level. The findings show that having an understanding of identity document (ID) theft can help address cybercrime since the nature of the crime is identified. The authors also indicated that using technology contributes to the occurrence of identity document theft which is often associated with the ignorance of the victims. The findings of this study pointed to the necessity for sustained and increased awareness in the Polokwane policing region to comprehend the causes of ID

theft. While the study revealed the extent to which identity theft has increased over the years, the study did not show its influence on firm performance, a gap, that the current study intended to address.

Piquero et al., (2021) used a focus group discussion to assess the use of dark web scanning, biometric scanning, and subscription-based monitoring programs as technical solutions in the identification of identity theft crimes. The author gathered data by coordinating with the Identity Theft Resource Center (ITRC) and ten professional conferences whose aim was to address identity-based crime victimization. The participants of the research provided a common perspective concerning the current cyber threats that face the business world and the consumers whose personal information is at threat of being stolen and used to commit fraud. According to the study, the business environment is ever-changing with organizations having to change their techniques to deal with criminals who are well-educated about the organizations and customers they are targeting. The study suggested that organizations need to adopt effective technological tools to address identity theft.

Vanhee (2020) investigated how the use of preventative measures is impacted by financial loss and other detrimental effects of identity theft victimization. This study made use of the 2016 Identity Theft Supplement (ITS) of the National Crime Victimization Survey (NCVS). For the Bureau of Justice Statistics, the NCVS is a yearly cross-sectional self-report victimization survey. Identity theft is a challenge, according to the report, affecting millions of individuals annually resulting in billions of dollars in financial damages. Because the power of the police and other institutions to protect persons from these crimes is limited, people are frequently responsible for their protection. The study evaluated performance based on financial performance. This study operationalized performance into

financial and non-financial performance and establishes the effect of identity theft on the two measures of performance.

Chesimo's (2020) study looked into the elements that promote fraudulent transactions and their impact on NGOs' operational effectiveness in Nairobi County. The research relied on primary data collected via structured questionnaires. Slovin's formula was used to sample. The results of the factor analysis suggest that, while various fraud elements have an impact on NGOs' operational success, only restrictions and rationalizations are relevant. The study found that the top effects of fraudulent transactions identified were loss of potential sponsors, insolvency, failure to accomplish project objectives, and job loss among personnel. The constraint identified was due to the use of a questionnaire that encouraged anonymity, which could lead to completely dishonest replies.

Okeke (2015) did a study with the goal of preventing crimes linked to internal identity theft in the United Kingdom. The research objectives were fulfilled by implementing a qualitative case study technique. From 2011 to 2013, data was collected empirically throughout the northwest of the United Kingdom. Archival analysis, semi-structured interviews, and participant observation were used in the field study. According to the study's findings, online retail customers' credit/debit card information is vulnerable to internal identity theft-related crimes (IIDTRC), which go beyond issues like trade secrets and trademarks. Furthermore, the survey found that many preventive measures against IIDTRC are implemented without taking into account the function of management-based human-centered security, with the primary focus being on software security. The study however did not introduce the aspect of performance. This study filled the research gap by determining the effect identity theft had on SME performance.



### **2.2.3 Phishing and Performance**

Williams, Hinds, and Joinson (2018) investigated the susceptibility to phishing in the workplace. Employee opinions of their susceptibility to spear phishing and how they handle suspicious emails at work were investigated using a standardized question design. The study found that when it comes to employee susceptibility to spear phishing emails and phishing in general, it's critical to consider the larger work context. Workplace norms and routines were most likely a major factor determining response behavior, influencing the formation of context-specific habits, expectations, and risk perceptions. These factors influenced the information-processing processes employed when a suspicious email is received, as well as the email's subsequent success. From the findings, it can be drawn that phishing negatively affects performance as indicated by the disruption of information processes. However, the study was not clear in showing the correlation between phishing and performance, a key concern for the current study.

Iuga, Nurse, and Erola (2016) undertook a web-based study with 382 respondents to assess whether study variables can facilitate or hinder internet users in differentiating phishing pages from authentic pages. The authors looked into the link between people's demographics and their propensity to recognize phishing and time-related elements. Data about the cursor movements of the respondents was also gathered. The results showed that pop-up-related attacks had a higher success rate than other studied tactics, and that gender and length of PC use have statistically significant effects on phishing detection. The study discovered that employing anti-phishing tactics has a favorable effect on output.

Phishing or electronic fraud is a theft activity that can cost a corporation its savings, according to research by Esmat, Alharbi, and Karrar (2021). Phishing is a criminal activity

that uses the social engineering technique and is one of the most successful ways to deceive people who are not paying attention. Some professionals actively seek the information as a result of user experience, whereas many hackers use covert methods to steal customer personal data, by infecting user devices with malware. This study employs a quantitative methodology. There were 271 people in the study. The study revealed that the reduction of spear phishing was to improve good organizational practices. The study indicated that all organizations need to have anti-phishing practices to record high performance. Although the study was current, it only focused on one type of cybercrime while the current study focused on four cybercrimes: data breach, identity theft, phishing, and malware attack.

Abroshan, Devos, Poels, and Laermans (2021) looked into how styles of decision-making and risk-taking influence the probability of phishing victimization. The researcher collected data by requiring the respondents to play a risk-taking game and answering questions related to psychological scales to assess their behaviour before undertaking a simulated phishing campaign to evaluate their capacity of being phished across three selected phishing processes. The study discovered that users' ability to be phished in the various steps may be predicted by their risk-taking attitude and gender. Other direct and indirect behavioral aspects, on the other hand, can be studied in the future. The study results can be used to develop a framework for preventing phishing efforts from succeeding, starting with the fundamental causes. The study presented a study gap that was filled by the current research. The study did not indicate the direct relationship between phishing and performance, an objective of the current study.

#### **2.2.4 Malware Attacks and Performance**

To understand the issues affecting malware attacks, a study by Kumar, Ojha, and Srivastava, (2018) was conducted. Malware attack factors were found, and a model was proposed. To validate the proposed model, SEM (Structural Equation Modeling) was employed, and a regression analysis was done to determine the relevance of the detected components. The researchers looked at three types of malware: knowledge, negligence, and inadequate software protection. The study found that the most important aspect of malware attacks is an inadequate software protection and that this factor is directly linked to costing components. As a result, it is possible to conclude that greater financial control may aid in the prevention of malware assaults. It went on to say that, current anti-malware security is insufficient due to a lack of resources. A constant upgrade was required, which necessitated expenditure, and most businesses are unwilling to invest at this time. It was established that the greater the investment in malware security solutions, the lower the odds of becoming a victim of a malware attack. The study concentrated on the investment made in reducing the risk of malware attacks; the study did not show the impact malware attacks can have on performance, the specific objective of the current research.

A study by Silva, (2020) investigated malware attacks on organizations. The study used secondary data for analysis. The absence of reliable frequency monitoring and the effects of these types of cyber-attacks, according to the report, makes it difficult for the healthcare industry to properly safeguard its networks. The author indicated that the best approach for hospitals to safeguard themselves is to be proactive and take action to fix potential vulnerabilities and shortcomings. According to the researcher, hospitals should conduct risk assessments to better understand the magnitude of the risk of malware attacks on their

business, as well as the extent to which successful attacks might interrupt operations. The study noted that malware attacks negatively influence business operations which ultimately affect performance. The study was based on secondary data only; the researcher ought to have collected primary data to improve the validity of the data gathered.

A study by Lévesque, Chiasson, Somayaji, and Fernandez, (2018) examined the relationship between antivirus software, users, and malware. The study included 50 participants who agreed to use laptops to track malware attacks and collect information on user behavior during a four-month period. The study's conclusions on the efficiency of antivirus software and human risk factors were unexpected and counterintuitive. The study discovered that AV (Antivirus) performance was poorer in real-life situations compared to controlled ones. Furthermore, malware attacks were found to be significantly correlated with computer knowledge, network usage volume, and peer-to-peer activity. The researchers discovered a link between virus activity and performance. However, the focus of the study was on anti-virus performance; this study focused on the performance of the entire organization.

A study was done by Arunlal, (2019) on the impact of malware in modern society. Secondary data was used for analysis. According to the survey, cyber-attacks result in significant loss of business information and intellectual property, as well as damage to brand reputation and financial loss. The study found that, as the amount and technological sophistication of malware grows; present malware detection systems are insufficient to keep hackers out of the system. The study also indicated that cyberspace is an arms competition, with one side advancing human life and the other posing an increasing threat to the planet. According to the study, the performance of an organization can be affected

negatively as a result of malware attacks. The study only gathered secondary data; this research gathered primary and secondary data.

Malware is one of the most serious risks to system security and company performance, with malware and spam causing complicated system challenges. AlMarri (2017) did a study to look into the numerous complexities that investigators confront when it comes to malware detection and analysis. To arrive at a successful result, the study used a unique cross-referencing method in which all alternatives were gathered, investigated, and critically analyzed. According to the study, anti-forensic strategies are often used by malware to escape inquiry and detection. Additionally, as a result of inadequate tools, the outcomes of assessing these attacks are often ineffectual and may bring up challenges to getting efficient evidence. The study presented a study gap since it did not indicate the influence of malware attacks on firm performance, as the current study intended to do.

### **2.2.5 Role of Kenyan Government in Cyber Security**

Cybercrime has grown as a major threat around the world, and Kenya is no different. The frequency and sophistication of cyberattacks in the country have steadily increased. To fight this expanding threat, Kenya's government has implemented a number of regulations and programs aimed at combating cybercrime and improving cybersecurity within its borders. One of the pivotal initiatives in Kenya's fight against cybercrime is the National Cybersecurity Strategy (NCSS), introduced in 2014. The NCSS is a complete framework that includes cyber incident prevention, detection, response, and recovery (Communications Authority of Kenya, 2014). It highlights the significance of collaboration among government institutions, the commercial sector, and civil society in improving Kenya's overall cybersecurity posture.

Kenya's government passed the Computer and Cybercrimes Act in 2018, marking a key legislative milestone in the country's cybersecurity landscape. This Act establishes a legislative framework for combating cybercrime by criminalizing activities such as hacking, identity theft, and online fraud and imposing fines on violators (Republic of Kenya, 2018). It also creates the National Computer and Cybercrime Coordination Committee, which is in charge of overseeing the Act's enforcement and implementation. Kenya formed the Kenya Computer Incident Response Team (KE-CIRT) to strengthen its capabilities in dealing with cyber incidents (Ouma, 2021). The Communications Authority of Kenya works with a variety of stakeholders to improve incident reporting and information exchange. Simultaneously, the government has been investing in cybersecurity training and education in order to develop a competent workforce capable of effectively mitigating cyber risks.

Despite these admirable efforts, Kenya confronts a number of obstacles in combating cybercrime completely. The ineffective execution of cybersecurity measures is hampered by resource restrictions such as low budget, a shortage of experienced workers, and outdated technical infrastructure. Furthermore, there is an urgent need to enhance public awareness about the dangers of cyber-attacks and the precautions that individuals and organizations should take (Richards, N. U., & Eboibi, 2021). Cross-border issues are another big impediment. Cybercriminals regularly operate beyond national borders, making efficient tracking and prosecution challenging. As a result, international cooperation is critical in dealing with these transnational challenges. Furthermore, striking the correct balance between cybersecurity efforts and people' right to privacy is a

continuing challenge that necessitates careful thought in policy creation and implementation.

### **2.3 Theoretical Framework**

This study is best anchored by the Routine Active theory that aims to explain the existence of crime and in this case, cybercrime. The routine activity theory was proposed by Cohen and Felson in 1979 to account why crime rates increased in the 1960s and 1970s despite better income levels and standard of living in American society. According to Cohen and Felson (1979), the differences in the rate of crime were attributed to the changes in daily activities. The authors argued that although there were changes in the structural conditions that motivate criminals, the daily routine changes facilitate the convergence of a motivated criminal, absence of security, and suitable target. In other words, rising crime rates are caused by an increase in the number of opportunities for crime to take place and not by a rise in the number of criminals in society. Additionally, they contend that rather than having an additive effect on crime rates, the possibilities that arise as a result of the convergence of the three factors have a ripple effect. As a result, the solution to the rising rate of crime ought to be identified in the situational structures where crime is evidenced (Cohen & Felson, 1979).

In essence, the routine activity theory describes how crime takes place when three elements converge: a motivated criminal, absence of security, and a suitable target. Crime occurs when these elements come together in space and time. Essentially, the convergence of these three elements enhances the possibility of criminal victimization and creates chances for criminal and deviant activities. The exclusion of any of these three factors from the equation precludes criminal and deviant behavior from occurring (Yucedal, 2010). A

motivated criminal might not be able to spot a criminal opportunity, claim Mustain and Tewsbury (1998). An offender may not be able to locate a vulnerable or valuable person or property to awaken his or her attention. The perpetrator may discover a good target, but because it is properly guarded, he or she may not be able to commit a criminal act.

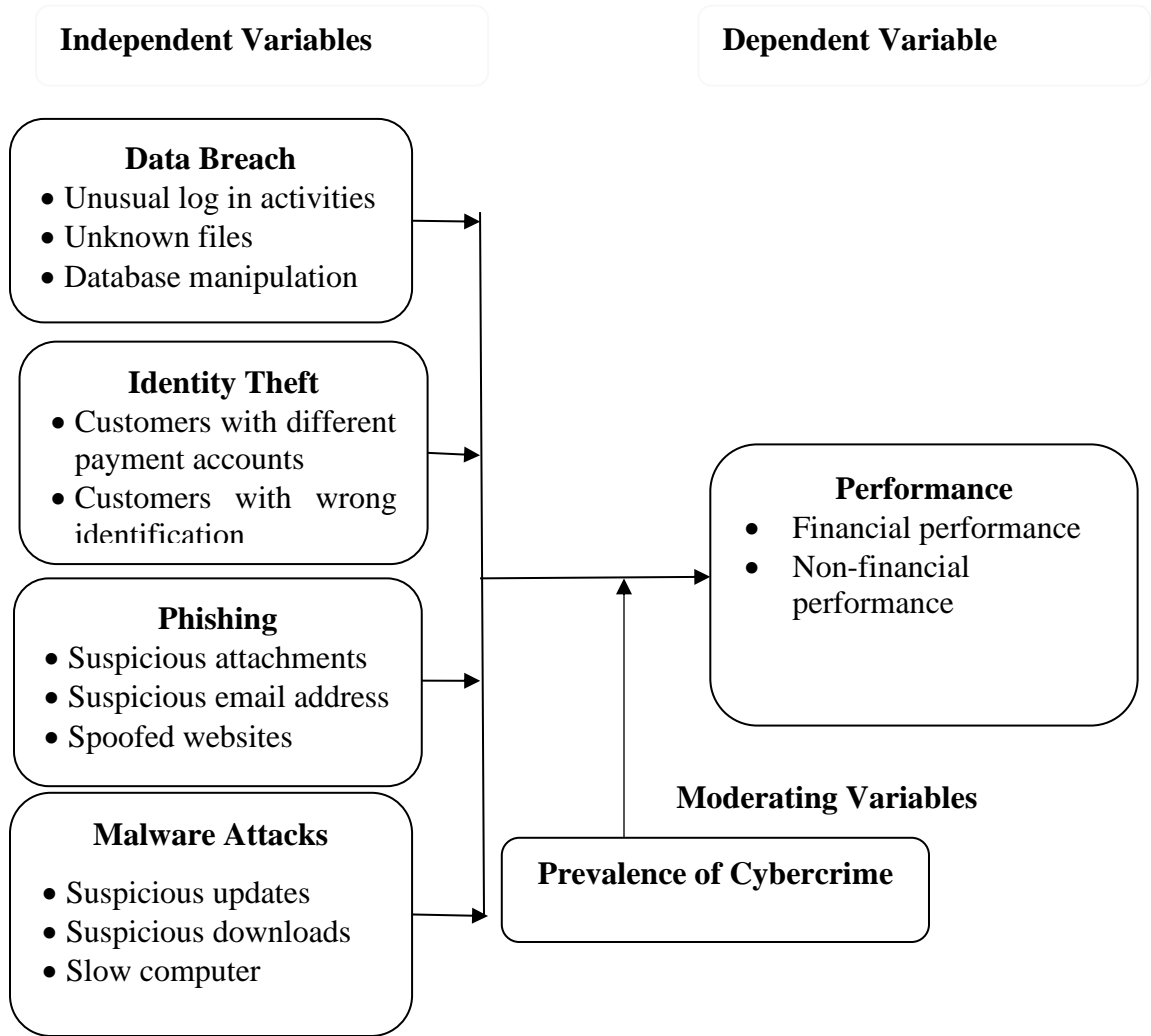
According to routine activity theory, criminals' incentives for committing any crime are different (ranging from enjoyment, monetary value, and revenge), but in the absence of a crime opportunity, these motivations are inadequate to successfully drive the criminal thought into action. Scholars such as Clarke and Felso (1993) agree that there is a need to understand the motivation of criminals and the conditions that drive criminal intentions into actions (Yucedal, 2010). The authors claim that understanding the situations that drive crime is essential in preventing crimes by changing the conditions.

This theory applies to the study since it illustrates the chances for cybercrime. According to the theory's presumptions, SMEs are more susceptible to cybercrime than large organizations since they pay less attention to guaranteeing cyber security. This is supported by Wekunda (2015). Moreover, some SMEs generate a lot of income, a motivation that may drive criminals to engage in cybercrime targeting such businesses. Therefore, based on the assumptions of the routine active theory, it is likely that SMEs have fallen victim to cybercrime, therefore, grounded on this theory, this study sought to determine the effect these cybercrimes had on the performance of SMEs in Nairobi, Kenya.

## **2.5 Conceptual Framework**

Figure 1.1 illustrates the study variables presented on a conceptual model. The model showed the link between cybercrime (Data breach, identity theft, phishing, and malware attacks) and performance.





**Figure 1. 1:** Conceptual Framework

## **CHAPTER THREE: RESEARCH METHODOLOGY**

### **3.1 Introduction**

This chapter describes the procedures used to carry out the study in the field. It describes the research strategy, data type and source, target population, sampling methods and procedures utilized to collect data, and data analysis.

### **3.2 Research Design**

Berger and Torres (2016) describe a research design as a blueprint adopted during research that aims at providing answers to the research question and facilitates making a summary of study findings. The study used a cross-sectional descriptive research methodology, which allowed for the collection of data at the same time. This strategy improves data gathering efficiency by capturing information in a uniform and succinct period. This type of research design also allowed the researcher to provide a better description of the study variables that is cybercrime and performance.

### **3.3 Target Population**

The Kamukunji Constituency in Nairobi County was chosen as the venue for the study on SME owners due to its distinctive qualities and strategic location. This area is home to a significant number of small and medium-sized firms (SMEs), according to Githuku (2019), who reports the presence of 5,277 SMEs. The Kamukunji Constituency's proximity to Nairobi's core business sector improves accessibility, making it a suitable place for undertaking extensive research. The ease with which this area can be reached enables for effective data collecting and contact with a wide range of business owners.

The Kamukunji Constituency's SME environment is remarkably broad, covering a wide range of industries such as clothes retail, hotel, hardware, steel, and furniture. This diversity

extends not only to the sorts of enterprises but also to the SME owners' backgrounds. The target population's complex character provides a rich and diverse sample for the investigation. Engaging with owners from these many sectors enables the examination of various market dynamics and difficulties. This comprehensive methodology allows for a more in-depth study of the SME ecosystem in a city like Nairobi. The diversified character of the SMEs in Kamukunji Constituency consequently provides a valuable microcosm for investigating the broader difficulties and opportunities confronting Kenya's small and medium-sized firms.

The study obtained data from the owners of enterprises in the SME sector since they are familiar with the day-to-day operations of their businesses and so have insights into how cybercrime has impacted the performance of the SMEs. Cybercrime is often conducted by outsiders seeking to target larger corporations. Thus, the cybercriminals use SMEs as a conduit in their pursuit of targeting larger corporations which are in business with the SMEs. It is easier for cybercriminals to target SMEs, since they do not take the issue of cyber security as seriously as the larger corporations. This leaves a gap for cybercriminals to use SMEs as a means to an end hence affecting the SMEs' business operations.

Additionally, the study collected data from four (IT) Information Technology experts from two companies: Cyber Security Africa and Enovise Limited (two IT officials from each company). The study targeted the two IT companies since they work hand in hand with different companies to ensure cyber security. The study targeted IT officials since they were in a position to offer in-depth data on cybercrime and make recommendations for the best cyber security solutions for SMEs.

### 3.4 Sample Design

Cooper and Schindler (2011) used a basic random sample approach to ensure that every participant had an equal opportunity to contribute to the study. This approach was deemed appropriate since it allowed for the random selection of businesses, reducing the possibility of biased sampling and improving the study's overall neutrality. The Krejcie and Morgan (1970) formula was used to obtain a sample size.

$$S = \frac{X^2 NP(1-P)}{d^2(N-1) + X^2 P(1-p)}$$

where s = Sample.

$X^2$  = the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841).

N = target population.

P = the population proportion (assumed to be .50 since this would provide the maximum sample size).

d = the degree of accuracy expressed as a proportion (.05).

A total of 358 SME owners in Kamukunji constituency made up the sample size of the study. Additionally, the researcher purposively sampled four IT specialists/experts from Cyber Security Africa and Enovise Limited. Therefore, the sample population for the study was 362 respondents (358 SME owners in Kamukunji consistency and four IT specialists/experts).

### **3.5 Data Collection Methods**

#### **3.5.1 Surveys**

The study gathered quantitative data by conducting surveys. The semi-structured questionnaire was used to gather primary data from the 358 SMEs' owners. The researcher sought the help of two research assistants to administer the questionnaires to each of the SMEs owners. This facilitated easier and faster collection of data. The research assistants were trained on the objective of the study and the importance of conducting the study. The researcher together with the research assistants administered the research questionnaires using the drop and pick technique. The researcher together with the research assistants administered the questionnaires to the SMEs owners and picked them later after a week. This allowed the SME owners to have adequate time to answer the research questions. The researcher and research assistants made phone calls to remind the SME owners to fill in the questionnaires. This ensured that adequate data is gathered for the study.

#### **3.5.2 Key Informant Interviews**

The researcher scheduled key informant interviews (KIIs) with the four IT specialists (two from Cyber Security Africa and two from Enovise Limited). The KIIs were scheduled at the convenience of the IT specialists. The researcher made appointments with the IT specialists. The KIIs were conducted at the offices of the IT specialists. This ensured that the key informants were comfortable to offer the necessary information with reference to the study objectives. Moreover, the researcher created a rapport with the interviewees to facilitate easier communication. The interviews took approximately 20-30 minutes.

### **3.5.3 Observations**

The researcher made observations while visiting the SMEs in Kamukunji. The researchers observed the day-to-day operations of the SMEs with a key focus on the use of technology in the SMEs. The researcher made observations of the SMEs after seeking permission from the owners of the business.

### **3.5.4 Desk Review**

The researcher complemented the data collection by collecting secondary data on the general concept of cybercrime as experienced by SMEs. The researcher conducted a desk review to gather secondary data from existing documentations such as journals, books and reports.

## **3.6 Data Collection Tools**

The study took a dual approach, collecting both quantitative and qualitative data. Questionnaires, a guide for key informant interviews, and an analysis of secondary data sources were used as data gathering instruments.

### **3.6.1 Questionnaire**

A semi-structured questionnaire was developed to gather primary data. The use of semi-structured questions helped in evaluating and investigating the influence of cybercrime on performance in SMEs in Kamukunji constituency in Nairobi County. The questionnaire was categorized into two sections. Section A gathered demographic data about the owners of the SMEs in Kamukunji constituency; section B and C contained questions related to the study variables that facilitated in answering the research questions.

### **3.6.2 Key Informant Interview Guide**

Qualitative data was collected using an interview guide to collect information from four IT experts from Cyber Security Africa and Enovise Limited. The researcher conducted interviews with the four IT specialists since they understand cybercrime and cyber security, thus was critical in offering invaluable information about the study variables. The interview guide was open-ended allowing the interviewees to offer as much information as they could in regard to cybercrime in SMEs.

### **3.6.3 Secondary Sources of Data**

Secondary data was gathered to complement the study. The secondary data was collected from existing publications such as journals, reports, books, and articles.

### **3.7 Pilot Study**

A pilot study is vital because it enhances reliability and determines the instruments to be used without any contamination of the research respondents before gathering the data that was used for the study. A 10% of the study population was included in the pilot test. The pilot study was conducted in Nairobi CBD since it contains SME operators as well. The importance of a pilot study is to test the research tools in case of any weaknesses and check for clarity and precision of items in the questionnaires. Further piloting enables the researcher to get feedback from pilot respondents on specific tools requiring moderation and further refining and informing the same of the research.

#### **3.7.1 Validity of the Research Instruments**

The level to which the gathered data can assess what it was intended to measure is known as validity. Content validity and face validity was used in this investigation. Content validity was assessed to ensure that all key features of the study's variables are included. A

pilot test was undertaken to determine content validity. The pilot test identified the research instrument's flaws, which was addressed to develop the research items to be used in the final data collection. Face validity of the research items was measured by having one-on-one discussions with the academic supervisors on the appropriateness of the research tool. Discussions were held with the academic supervisors to improve the research tools.

### **3.7.2 Reliability of the Research Instruments**

According to Sekaran and Bougie (2016), a study's reliability is determined by the replicability and consistency of measurement based on data collecting and analysis methods. To assess data reliability, a test-retest tool was utilized. Cronbach's Alpha reliability test was used to measure scale reliability. The researcher conducted a pilot test to ensure the internal consistency of the research items. Bryman (2011) argues that pretesting the research instrument with appropriate respondents helps in identifying gaps not covered by the research tool. Cronbach's alpha ( $\alpha$ ) was used to calculate this reliability measure. According to Nunnally (1978), instruments used in research should have dependability of 0.70 or above.

## **3.8 Data Analysis**

### **3.8.1 Quantitative Data Analysis**

The quantitative data was evaluated using descriptive and inferential statistical approaches. The quantitative data gathered from the questionnaire in this study were analyzed using the Statistical Package for Social Scientists (SPSS) version 25.0. To identify the study variables and assess the quantitative data, descriptive statistics such as frequencies were used. Linear regression analysis was used in the study of the influence of cybercrime on the performance of SMEs in Nairobi, Kenya. The composite scores for both variables were



generated in this investigation. The cybercrime composite score was calculated by averaging the dimensions of the crime, which included data breach, identity theft, phishing, and malware attack. Similarly, the performance composite score was calculated by averaging the mean scores of its aspects, which included financial and non-financial performance. The regression model took the following form.

$$Y = a + bx_1 + e$$

Where; Y= Performance composite score

X<sub>1</sub>= Cybercrime score

b= Regression coefficient

e = Error term.

The model was used to test the hypothesis proposed in this study with a 95% confidence level, and the null hypothesis was rejected when the p-value associated with the regression coefficient fell below 0.05.

### **3.8.2 Qualitative Data Analysis**

Content analysis was used to analyze the qualitative data acquired through the interview guide and open-ended questions, as defined by Creswell and Miller (2000). This qualitative data analysis procedure includes taking notes, which may include handwritten notes, observations, and tape recordings. The researcher made handwritten notes and taped the sessions during the interviews, eventually transforming the notes into intelligible write-ups. Three major phases were included in the qualitative data analysis. There was an initial

phase devoted to digesting the obtained data, focusing on analysis, and organizing the material into themes.

Following the interviews, the researcher carefully listened to the recorded sessions and meticulously reviewed all participant responses in order to acquire a clear knowledge of the insights linked to the interview guide. Wilson (2012) suggests that the researcher organize the information into appropriate categories, known as themes, to ensure clarity in presenting the findings. For coding the acquired data, the analysis used a manual thematic analysis method. The development of a theme is the outcome of categorization, coding, or analytical contemplation. The researcher paid close attention to the chosen words when developing respective codes to assure the accuracy of the produced themes. The qualitative data was presented in a narrative fashion, which allowed for direct quotations from study participants.

### **3.9 Ethical Considerations**

The researcher took the obligation of ensuring that ethical considerations are upheld. The researcher obtained a NACOSTI permit allowing for the research to be conducted. In addition, a letter of introduction from the learning institution was obtained approving the research. All the respondents participating in the study volunteered after granting their consent. The researcher did not coerce or offer any incentives to the respondents to take part in the study. The researcher educated the respondents on the objectives of the study and assured them that confidentiality would be maintained. Moreover, the data gathered was used for academic purposes only.

## CHAPTER FOUR: DATA ANALYSIS AND PRESENTATION

### 4.1 Introduction

This chapter includes a review of the data that was gathered, its subsequent presentation, and an in-depth analysis of the results. The participants' response rate and the relevant demographic information are covered in depth in the first section. The specific objectives serve as the primary foundation for the presentation of the findings.

### 4.2 Demographic Information

The study sought to compile the demographic data on the SME owners who took part in the research. Before gathering information on the study variables, the researcher aimed to ascertain the demographics of the sampled SME owners. The gender, age, and level of education were among the demographic data collected.

#### 4.2.1 Demographic Information of the SME owners

Data on the gender of the sampled SMEs owners was collected. This was important since it provided a better understanding into the gender dynamics in SMEs ownership in Kamukunji constituency in Kenya. The findings were presented in Table 4.1.

**Table 4.1: Gender**

Gender	Frequency	Percentage
Male	194	64.0
Female	109	36.0
<b>Total</b>	<b>303</b>	<b>100</b>

**Source: Primary Data (2023)**

Table 4.1 showed that 64.0% of the SME owners were male while 36.0% were female. Based on the findings, in Kamukunji area, there are more male entrepreneurs unlike female entrepreneurs. However, the finding suggests that more women are stepping up to start their own businesses.

The researcher also sought to identify the age of the owners of the sampled SMEs. The age provided are distributed in age groups to facilitate easier data analysis. The results were shown in Table 4.2.

**Table 4.1: Age of SME owners**

<b>Age</b>	<b>No. of respondent</b>	<b>Percentage</b>
Below 20 years	9	3.0
20 -30 years	37	12.2
31 - 40 years	152	50.2
41- 50 years	87	28.7
Above 50 years	18	5.9
<b>Total</b>	<b>303</b>	<b>100</b>

**Source: Field data, (2023)**

Table 4.2 showed that most of the SME owners who owned SMEs in Kamukunji constituency were aged 31-40 years. This may be attributed to the fact that at this age, majority of the individuals have already identified what they would like to do to earn a living and are willing to take risks, especially in business. Moreover, the findings show that only nine (3%) of the SME owners were aged 20 and below. This is attributed to the fact that at this age, most of the individuals are still in school. Based on the findings, it was discovered that individuals aged 30 years and above are willing to take risks by venturing

into business. Moreover, at this age, the individuals possess relevant skills acquired in their 20s that can help propel the business.

The researcher also collected data on the level of education of the SME owners. This information was critical since it helped in understanding the SME owners especially with reference to their understanding of cyber-crime. The results were shown in Table 4.2 below.

**Table 4.2: Level of Education**

<b>Level of Education</b>	<b>No. of respondent</b>	<b>Percentage</b>
No formal education	23	7.6
Primary level	20	6.6
Secondary	43	14.2
College level	107	35.3
University level	89	29.4
Post-graduate	21	6.9
<b>Total</b>	<b>303</b>	<b>100</b>

**Source: Field data, (2023)**

Table 4.3 showed that majority of the SME owners had attained either a college level of education (35.3%) of a university level of education (29.4%). Only 7.6% of the SME owners did not have any formal education. The findings revealed that majority of the SME owners had attained the basic level of education. This was essential, since it implies that most of the SME owners understood the intricacies of running a business.

### 4.3 Profiles of the SMESs

Further, the researcher collected information on the length of time SMEs had been in operation in Kamukunji Constituency. The findings were as shown in Table 4.4.

**Table 4.3: Time in Operation**

<b>Time in Operation</b>	<b>Frequency</b>	<b>Percentage</b>
Below 1 year	3	1.0
1 – 5 years	127	41.9
6 – 10 years	79	26.1
11 – 15 years	54	17.8
16 – 20 years	32	10.6
Over 20 years	8	2.6
<b>Total</b>	<b>303</b>	<b>100</b>

**Source: Field data, (2023)**

The results presented in Table 4.4 showed that majority of the sampled SMEs (41.9%) had been in operation for a period of 1-5 years. This is the most sensitive time for any business. This is because; this period is often associated with the growth stage of a business, where the SMEs is working towards attaining its highest growth possible. Based on the findings 57.9% of the sampled SMEs sample for the study were over 5 years old. This implies that the business owners had stayed in the business environment for a definitive time, hence could provide in depth insights especially with reference to cyber-crime and its effects on performance.

The researcher also sought to identify the frequency to which the sampled SMEs in Kamukunji constituency in Kenya used technology. This is to better understand the extent

to which the sampled SMEs were vulnerable to cyber-crime as a result of the frequency in the use of technology by these businesses. The results were shown in Table 4.5 below.

**Table 4.4: Frequency of Using Technology Devices**

<b>Frequency of Use of Technology Devices</b>	<b>No. of respondent</b>	<b>Percentage</b>
Daily	303	100
Weekly	-	-
Not at all	-	-
<b>Total</b>	<b>303</b>	<b>100</b>

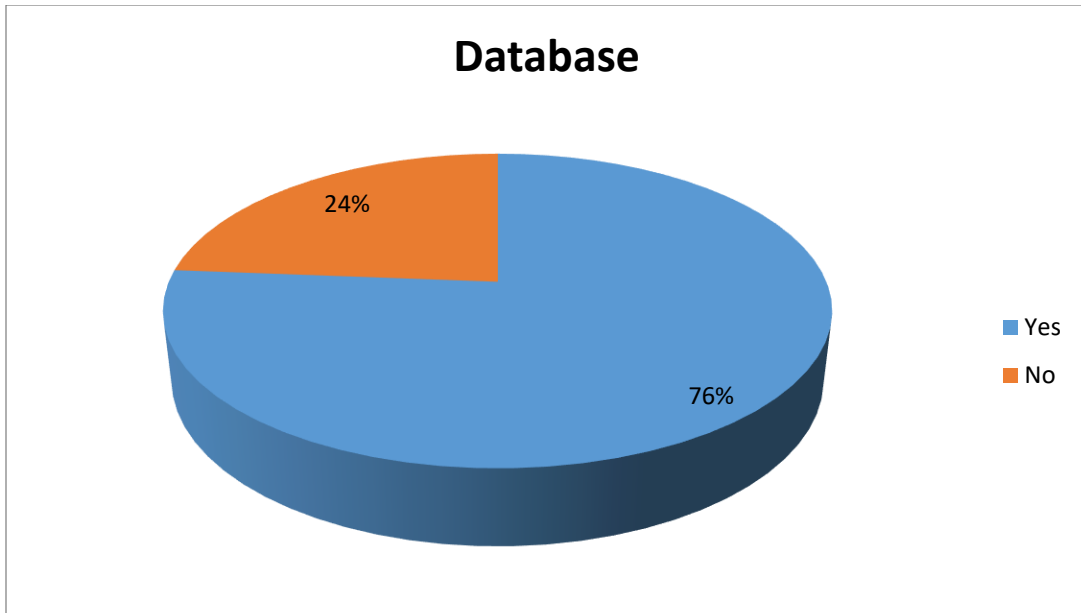
**Source: Field data, (2023)**

Table 4.5 showed that all the SME owners (100%) agreed that the SMEs used technology daily to facilitate their day-to-day operations. This was attributed to the mobile pay services where the businesses argue that a business in the modern world and in Kenya cannot be conducted without a phone.

#### **4.4 Descriptive Analysis**

##### **4.4.1 Data Breach**

The researcher sought to understand the concept of data breach from the perspective of the sampled SMEs' owners. The data are presented in Figure 4.1 below.



**Figure 4.1: SME’s Database**

**Source: Field Data, 2023**

Figure 4.1 showed that 76% of the sampled SMEs assessed had maintained a database while 24% of the sampled SMEs in Kamukunji constituency had not maintained a database. Based on the findings, the data collected was sufficient since majority of the sampled SMEs had databases, an implication of information and technology integration in the businesses. Further, the SMEs owners were asked to indicate the type of information recorded on the SME’s databases. This information was important to understand the type of information that is likely to be breached by cyber criminals. The findings were presented in Table 4.6 below.



**Table 4.5: Type of Information Recorded on the Databases**

<b>Type of Information</b>	<b>Frequency</b>	<b>Percentage</b>
Customer's information	203	87.9
Suppliers' information	127	54.9
Customer orders	218	94.3
Customer purchases	189	81.8
Daily sales	154	66.7
Transactions made	62	26.8

**Source (Field Data, 2023)**

Table 4.6 above showed that 203 of the SME owners agreed that customer's information was often recorded on the SMEs databases. Moreover, customer orders and customer purchases were also identified to be among the most recorded data on the database as agreed by 218 and 189 of the SME owners. This finding underscored the significance of tracking and documenting customer orders to facilitate order fulfillment, inventory management, and customer service. These findings suggested that the SMEs under study prioritized the collection and storage of customer-related data, which could include personal details, contact information, and preferences. The results thus support the notion that data breaches can significantly affect consumer behavior, which in turn can affect SME success. According to Janakiraman, Lim, and Rishika (2018), prioritization of customer data in SMEs indicates that maintaining data security is not only about protecting customer information but also about preserving customer trust and loyalty, which are critical for ongoing business success.

This strategy is consistent with a broader understanding of customer relationship management (CRM) in the context of small and medium-sized businesses. CRM strategies that are effective, such as rigorous recording of client orders and preferences, are critical for order fulfillment, inventory management, and improving customer service. These approaches not only improve business operations but also increase consumer loyalty and pleasure. Furthermore, the emphasis on keeping customer-related data, such as personal information, contact information, and preferences, demonstrates SMEs' rising appreciation for the usefulness of data-driven tactics. Janakiraman, Lim, and Rishika (2018) research supports this viewpoint by indicating that consumers tend to transfer from hacked to secure channels. Their research focuses on the consequences of data security breaches and the resulting changes in consumer behavior. This implies that SMEs must invest in comprehensive data security solutions to protect client information and keep their competitive edge.

The SMEs under study also recognized the importance of maintaining records related to their suppliers, potentially including contact details, contractual agreements, and transaction histories. This was evidenced by 127 of the SME owners agreeing that supplier's information was recorded on the databases. Moreover, during the data collection through observations, the researcher observed that the SMEs owners recorded the details of all of their customers to keep track of the transactions being conducted. The researcher saw the SMEs' owners making records on invoice books, stock record, and receipt books.

The information that received the lowest ranking was the daily sales and the transactions made as indicated by 154 and 62 respectively. Notably, while the two types of information was not agreed upon by majority of the SME owners, it is important to understand that the

daily sales and transactions made can inform decision-making processes, such as inventory management, pricing strategies, and revenue forecasting. Hence can be valuable information to cyber criminals in identifying which SMEs to attack. This is comparable to Juma'h and Alnsour's (2020) observation on the economic implications of data breaches. If daily sales and transaction data are not sufficiently protected and hence compromised, it can have a direct influence on financial performance measures like solvency and profitability. SME underemphasis on this data may raise them susceptible to attacks with serious financial ramifications.

The SME owners were also asked to indicate the person(s) had access to the data base. The results were presented in Table 4.7.

**Table 4.6 Access to the SME Database**

<b>Type of Information</b>	<b>Frequency</b>	<b>Percentage</b>
SME owner	154	50.8
Manager	123	40.6
IT staff	26	8.6
<b>Total</b>	<b>271</b>	<b>100</b>

**Source: Field Data (2023)**

Table 4.7 showed that 50.8% of the sampled SMEs owners interviewed had access to the databases. This indicates that SME owners, who are typically the primary decision-makers and stakeholders in the organization, were granted significant access to the database. This level of access was expected, as SME owners are responsible for overseeing all aspects of the business, including data management and decision-making processes that rely on accessing and analyzing the data. Managers were also found to have access to the SME database, although at a slightly lower frequency of 40.6%. Managers are key personnel responsible for various operational and strategic functions within the organization.

Granting them access to the database allows them to retrieve and utilize relevant information for decision-making, resource allocation, and monitoring purposes. The slightly lower frequency compared to SME owners could indicate that not all managers have equal access or that access privileges are tailored based on their specific roles and responsibilities.

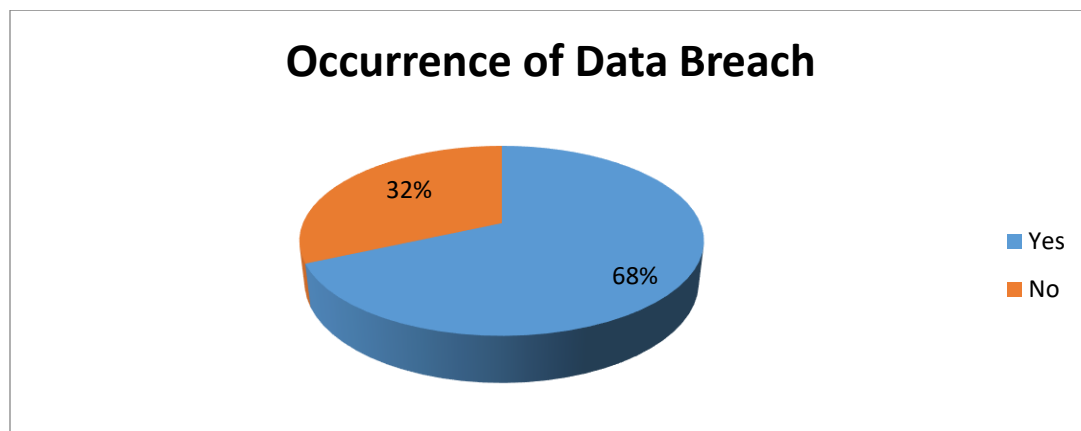
Knight's (2020) research underlines the societal benefits of establishing strong data security procedures in SMEs. This study is especially pertinent in light of the fact that SME owners and managers are the most frequent users of databases, giving them direct access to a variety of sensitive information such as financial records and consumer contact information. Sensitive access highlights SME leaders' vital role in preserving sensitive data, not only to preserve their business interests but also to maintain customer trust and societal trust in digital transactions. As shown in Knight's (2020) analysis, the frequent targeting of bank records and customer contact information by hackers is a major source of concern. Financial data is a company's lifeblood, providing insights into its operational health and strategic direction. When such data is compromised, it can have serious financial consequences as well as strategic implications. Furthermore, client contact information is a goldmine for cybercriminals, with numerous routes for further exploitation ranging from identity theft to targeted phishing assaults.

Gadirova's (2021) findings are consistent with Knight's (2020) observations, especially when it comes to the targeting of customer contact information in data breaches. Gadirova's research demonstrates the practical consequences of such breaches, proving that they can result in major changes in a company's financial plans, particularly in cash holdings and asset management. The emphasis on consumer contact information in cyber-attacks

highlights the twofold threat that SMEs face: not only do these breaches have a financial impact on the company, but they also destroy customer trust, which can have long-term ramifications for business survival and success.

In contrast, IT staff had the lowest frequency of access to the database, with only 26 cases reported. IT staff typically possess specialized technical knowledge and skills required to manage and maintain the SME's information systems and databases. Their access to the database is crucial for tasks such as database administration, system updates, security protocols, and troubleshooting. The relatively lower frequency of IT staff access was attributed to the fact that their primary role is to ensure the smooth functioning and security of the database rather than utilizing it for operational or managerial purposes.

The SME owners were asked to indicate whether the SMEs had ever experienced any form of data breach. The findings were shown in Figure 4.2.



**Figure 4.2: Occurrence of Data Breach**

**Source: Field Data (2023)**

Figure 4.2 above showed that 68% of the SME owners had experienced data breach. On the other hand, 32% of the sampled SMEs sampled had not experienced any form of data

breach. Based on the data collected, it was evident that data breach is one of the challenges experienced by SMEs in Kenya. This calls for better cyber security strategies to ensure that SMEs databases are safe and secure. These repercussions imply that data breaches may negatively impact SMEs' operations and results. This finding is consistent with Juma'h and Alnsour's (2020) findings, which revealed a drop in performance after a data breach. As a result, the findings highlight the importance of putting in place strong cyber security safeguards to safeguard SME databases and lessen the negative effects on performance.

Based on the data collected above, the SME owners were asked to indicate the information that was stolen from their databases. This was critical in understanding the type of information that cyber criminals are interested in especially with reference to SMEs. The findings were presented in Table 4.8.

**Table 4. 7: Type of Information Stolen from the SME Database**

<b>Type of Information</b>	<b>Frequency</b>	<b>Percentage</b>
Client's Contacts	201	87.1
Financial Records	175	84.5
Supplier's contacts	143	69.1
Investors contacts	23	11.1
SME inventory	87	42.0

**Source: Field Data (2023)**

According to the data collected, it was found that client's contacts (87.1%) were the most common type of information stolen. This was followed by the financial records (84.5%), supplier's contacts (69.1%), SME inventory (42.0%), and investor contacts (11.1%). The findings show that cyber criminals are primarily interested in obtaining client contact details, which could include personal information, email addresses, phone numbers, and other means of communication. The theft of client's contacts can have severe consequences for SMEs, as it not only compromises the privacy and security of their customers but also exposes them to potential phishing attempts, identity theft, and other fraudulent activities.

Financial records were also identified as a significant target for cyber criminals, with a frequency of 175. This finding highlights the importance of securing financial data within SME databases. Financial records encompass a wide range of sensitive information, such as banking details, transaction histories, invoices, and payment records. The theft of financial records can lead to financial losses, unauthorized access to funds, and even reputational damage for the affected SMEs. This finding is consistent with Juma'h and Alnsour's (2020) research, which focuses on the economic effects of data breaches. According to their research, the theft of financial documents, which results in financial

losses and reputational damage, shows the direct influence on the solvency, profitability, and liquidity of SMEs. This link indicates how data breaches can harm a company's financial health, matching the reduction in performance shown in their study.

Supplier's contacts were reported as stolen in 143 instances. The theft of supplier contacts can disrupt supply chain relationships, compromise confidential business information, and potentially lead to issues such as unauthorized access to supplier accounts or attempts to impersonate suppliers. Theft of supplier connections can disrupt supply chain relationships, a problem raised in Gadirova (2021) research on the larger effects of data breaches. As Knight points out, ensuring data security in this area is critical for preserving corporate operations and defending against third-party dependency. Such breaches can have a domino effect on the business's operations as well as its social relationships.

SME inventory was reported as stolen in 87 instances. This indicates that cyber criminals target information related to the SME's inventory, such as stock levels, product details, pricing information, and other inventory-related data. The theft of inventory information has the potential to disrupt operations, impact sales and fulfillment processes, and potentially lead to issues such as counterfeiting or unauthorized distribution of products. The theft of investor's contacts was reported in 23 cases. While relatively less frequent, this finding highlights the potential vulnerability of investor-related information within SME databases. The vulnerability of investor-related information and the possibility of theft correspond to the societal and economic effects described in Juma'h and Alnsour's (2020) study. Investor relations are essential for corporate success, and failures in this area can have a substantial influence on the company's financial stability and investor trust.



Qualitative data was gathered from IT specialists. According to the four IT specialists sampled the owners of SMEs had little understanding of data breach. The IT specialist explained that the owners of the sampled SMEs perceived data breach as the process where an authorized person had access to specific information. Based on the IT experts, the data breach is commonly committed by unhappy employees with the aim of stealing clients and investors from their current employers.

The researcher asked the interviewees whether it was possible to recover all the information in case of a cyber-crime. The interviewees noted that in most cases they were able to recover SMEs information, if a back-up was put in place. However, in the event that there was no back up, the IT specialist stated that it would be challenging to retrieve all the information stolen. However, they revealed that in some instances following data breaches that were able to recover some bits of information. The IT specialist emphasized the importance of SMEs having a back-up for all their databases.

Additionally, the ICT specialists/experts revealed that the common perpetrators of cyber-crime are employees of SMEs. The interviewees argued that often the employees of SMEs have access to the business databases, hence easy for them to engage in data breach and identity theft. One of the IT specialist/experts said:

*“often, the employees in SMEs engage in cyber-crime against their own firms since they have access to information. Moreover, a key driver for engaging in cyber-crime is usually for monetary reasons.”*

(IT specialist/expert, 004)

According to IT experts, there is a misunderstanding among SME owners about data breaches, which are typically viewed as unlawful access to information. This perception is significant in light of Knight's (2020) results, which indicate a need for increased data security awareness and policy implementation. The internal threat created by disgruntled employees, as recognized by IT specialists, emphasizes the need of Knight's advocated comprehensive data protection solutions.

#### **4.4.2 Identity Theft**

The second goal of the study was to analyze the impact of identity theft on the performance of SMEs in Nairobi County, Kenya. Identity theft, as defined in this study, is the illegal acquisition of an individual's personal details, such as their name, address, social security number, or credit card information, for the purpose of committing fraud or indulging in other criminal acts. As a result, the researcher sought information from SME owners about persons within their organizations who had access to the contact lists of the selected SMEs. Table 4.9 summarizes the findings of this inquiry.

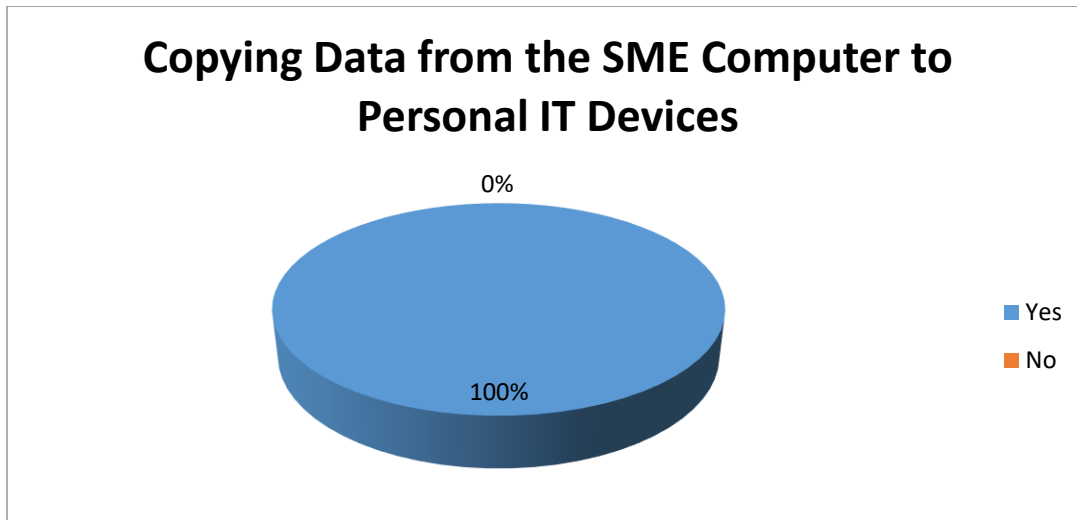
**Table 4.8: Personnel with Access to the SME Contact List**

<b>Personnel with Access to the SME Contact List</b>	<b>Frequency</b>	<b>Percentage</b>
SME owner	185	61.1
Manager	113	37.3
IT staff	5	1.6
<b>Total</b>	<b>303</b>	<b>100</b>

Source: Field Data (2023)

Table 4.9 showed that the personnel who had access to contact list in SMEs were the SME's owners (61.1%) followed by the management (37.3%). From the findings, it was revealed that very few IT personnel (1.6%) have access to the contact lists of the sampled SMEs. This finding is attributed to the fact that in SMEs, the owners hold the power and are involved in making close to all decisions surrounding the business; hence it only makes sense that they have access to the contact list. Moreover, it was revealed that managers, (37.3%) who work under the SMEs owner have a significant access to the contact list as they oversee the day-to-day operations of the businesses. Based on the study, it was revealed that only 1.6% of the IT personnel had access to the contact list. These data was expected since the IT personnel often engage in ensuring the cyber security of the business and not in maintaining the contact list of the business. Technology plays a key part in the facilitation of identity document theft, which frequently results from victims' ignorance, according to Rakololo and Maluleke (2020). These results highlight the need for SMEs to be aware of the threats posed by technology and train their staff on identity theft in order to stop internal breaches and protect sensitive data.

The SME owners were also asked to indicate whether the employees were allowed to copy any information from the SME's computers to their personal IT devices. Figure 4.3 showed the findings.



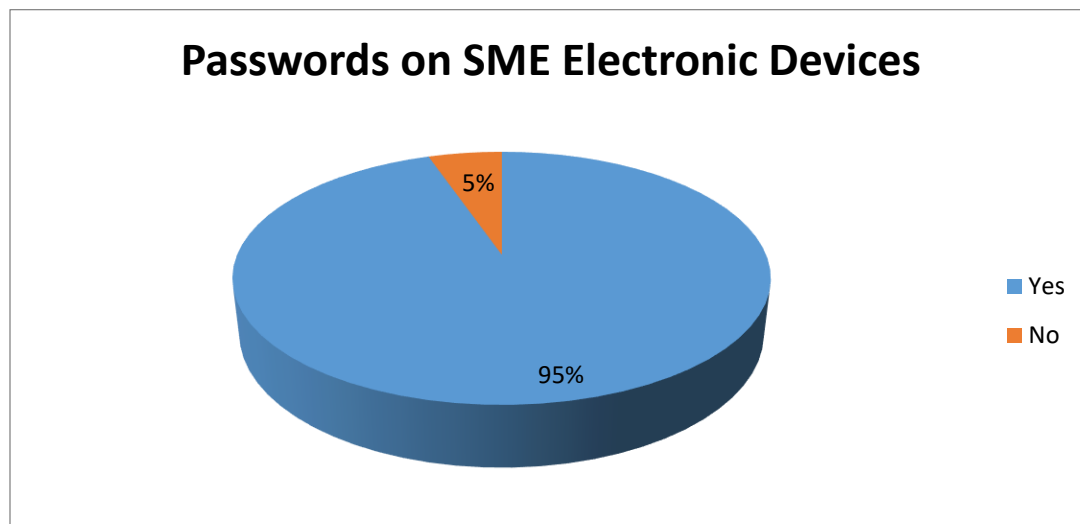
**Figure 4.3: Copying Data from the SME Computer to Personal IT Devices**

**Source: Field Data (2023)**

The findings presented in Figure 4.3 show that all of the SME owners (100%) agreed that no employee was allowed to copy any information from the SME computer to their personal IT devices. This measure is implemented in SMEs to deter the employees from being tempted to steal from the business. Moreover, this measure ensures that the SME information remains secure from perpetrators of cyber-crime. Piquero et al., (2021) underlines the importance of guarding against identity theft by limiting access to particular data or information within an organization and making sure that only pertinent individuals have authority. This backs up the study's conclusions that forbid employees from transferring data to their own devices, demonstrating a proactive strategy to prevent internal data breaches. SMEs can reduce the risk of unauthorized access and potential data

theft by putting in place procedures that prohibit such actions. These steps, along with the use of cutting-edge technological tools like biometric and dark web scanning, can improve SMEs' capacity to identify and stop identity theft.

Further, the researcher sought to understand whether the SME electronic devices have passwords. The results were shown in Figure 4.4 below.



**Figure 4.4: Passwords on SME Electronic Devices**      **Source: Field Data (2023)**

The results shown in Figure 4.4 show that majority of the sampled SMEs (95%) had passwords on all of their electronic devices. This was deemed important since it ensures that only authorized personnel have access to the information and data stored in the electronic devices. This was essential in deterring the employees of the sampled SMEs from engaging in identity theft. Vanhee (2020) established a significant connection between victims of identity theft and careless password management on computers. On basis of this discovery, the current survey finds that while majority of SMEs have password systems in place, there is a lack of consistency in password upgrades, potentially posing

vulnerability. According to Vanhee's (2020) research, SMEs should give cyber security practices like frequent password updates and strict password regulations top priority because of the financial costs associated with identity theft. SMEs can improve their overall performance and reduce the risk of financial losses due to identity theft by addressing this vulnerability.

The SME owners were asked to indicate how often the passwords on the SMEs' electronic devices were changed. The results were shown in Table 4.10.

**Table 4.9: Change of Passwords on SME Electronic Devices**

<b>Frequency</b>	<b>Frequency</b>	<b>Percentage</b>
Daily	0	0
Weekly	0	0
Monthly	25	8.3
When Needed	278	91.7
Never	0	0
<b>Total</b>	<b>303</b>	<b>100</b>

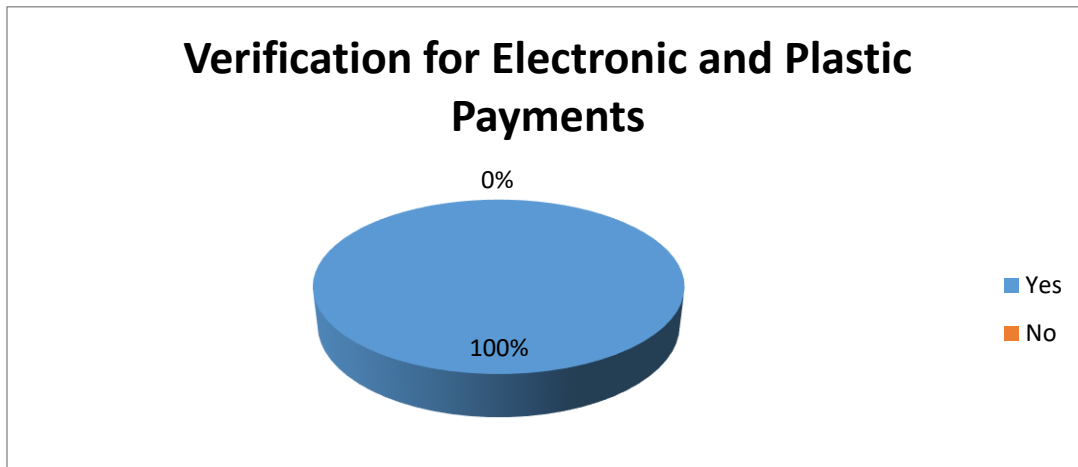
**Source: Field Data (2023)**

Table 4.10 showed that the sampled SMEs were not consistent in ensuring their cyber security. With reference to the data collected none of the sampled SMEs changed their passwords on a daily or even weekly basis. Only 8.3% changed their electronic devices passwords on a monthly basis. This is alarming since it means that access to the sampled SMEs electronic devices may be easy for identity thieves to prey on companies that are not keen on ensuring their cyber security. The findings revealed that 91.7% of the sampled SMEs changed their passwords when needed. This showed that the SMEs did not change

their passwords as often as necessary or even never if the businesses did not feel the need to do so. This finding is essential since it showed that a major reason for SMEs falling victim to cyber criminals is rooted from their laxity in ensuring cyber security through ensuring frequent password changes.

The researcher also sought to assess whether the SMEs employees were obligated to verify the identity of all customers who paid for purchases using electronic and plastic payment.

The results were presented in Figure 4.5.



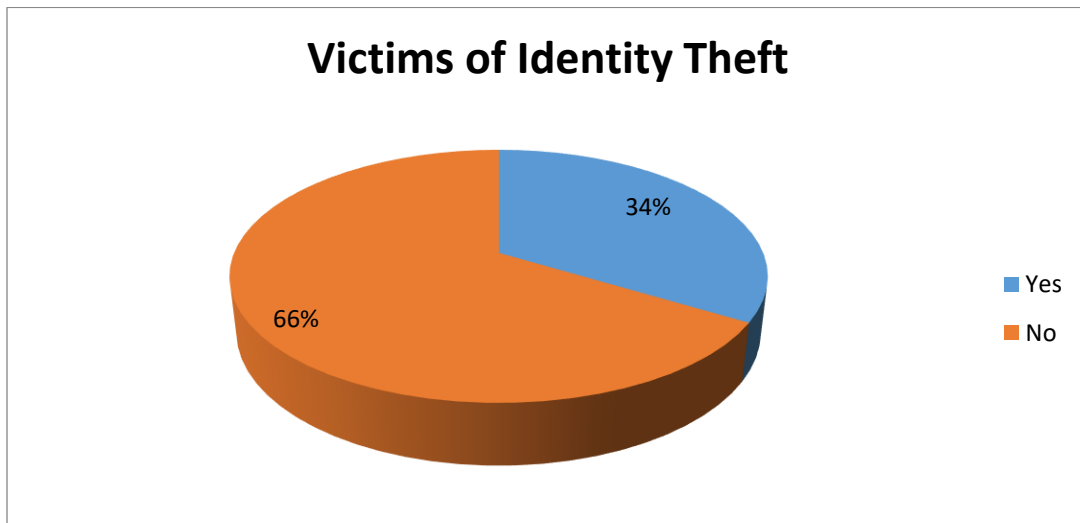
**Figure 4.5: Verification of Electronic and Plastic Payments**

**Source: Field Data (2023)**

According to Figure 4.5, it was revealed that the sampled SME employees' had the responsibility of verifying all electronic and plastic payments by requesting to see the identification of the customers making the purchases. This was also observed by the researcher while conducting observations of the SMEs in Kamukunji constituency. Through the observations, the researcher was able to see first-hand as the SMEs' employees verifying any electronic and plastic payments made by clients. This finding

resonates with results by Okeke (2015) who established that online retail customers' credit/debit card information is vulnerable to internal identity theft-related crimes (IIDTRC), which go beyond issues like trade secrets and trademarks. Therefore, it is potent to ensure that all electronic and plastic transactions are verified to avoid issues of identity theft.

To fully grasp the concept of identity theft from the perspective of the SME owners in Kamukunji constituency, the SME owners were asked to indicate whether the businesses had been victims of identity thieves, the results were shown in Figure 4.6.



**Figure 4.6: Victims of Identity Theft**

**Source: Field Data (2023)**

Figure 4.6 showed that majority of the samples SMEs (66%) had not fallen victim to identity theft while 34% of the sampled SMEs reported being victims of identity theft. The sampled SMEs that were victims of identity theft revealed that the incidences occurred as a result of the use of electronic and plastic payments where customers make purchases using other people MPESA accounts and debit/credit cards. The SME owners argued that



while globalization has paved way for increased use of electronic and plastic payments it presents a loophole to be exploited by cyber criminals.

The results of the current study, which show that 34% of the sampled SMEs polled reported incidences of identity theft, are consistent with those of Chesimo's (2020) study. Therefore, it is important to emphasize how susceptible SMEs are to these types of incidents. SME's may safeguard their operations and safeguard their stakeholders by putting in place strong cyber security measures, carrying out regular security audits, and teaching staff on how to spot and prevent identity theft. Okeke's (2015) research highlights the susceptibility of credit/debit card information of online retail clients to internal identity theft-related crimes. The current study emphasizes the significance of authenticating all electronic and plastic payments in order to stop consumer identity theft, which is in line with Okeke's (2015) findings.

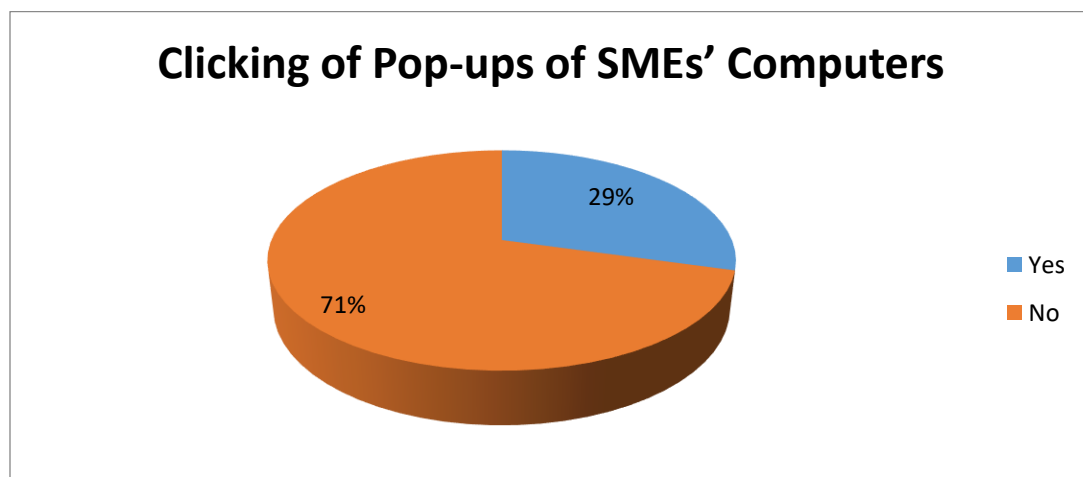
Qualitative data was collected from IT specialist/experts. The researcher sought to understand the perspective of the IT specialists/experts with regards to whether the owners of SMEs understood the concept of identity theft. The interviewees noted that the SMEs owners were knowledgeable on the concept of identity theft which resulted in the employees being vigilant by requesting identification from customers who made electronic and plastic payments.

The researcher collected qualitative data from four IT specialists to understand the common cybercrimes committed against SMEs. The four IT specialists revealed that identity theft was one of the common cybercrimes committed against SMEs. One of the interviewees revealed that due to the fact that people post their information online, it is easy for cyber criminals to steal the identity of customers. One of the interviewees noted that information

about people is readily available on social media platforms, hence, easy for cyber criminals to identify their target and phish for information. Further, one of the IT specialists said that the SMEs that fall victim to identity theft often lose their customers, hence lowering their performance. The finding resonates with results by Vanhee (2020) who found that identity theft is a challenge, according to the report, affecting millions of individuals annually resulting in billions of dollars in financial damages

#### 4.4.3 Phishing

The third goal of the study was to look into the influence of phishing on the performance of SMEs in Nairobi County, Kenya. For the purposes of this study, phishing was defined as the deceitful practice of sending phony emails, messages, or websites that appear to be from trusted sources in order to trick people into disclosing personal information or unknowingly installing malware. This definition was explained to the SME owners prior to collecting the data on phishing. The SME owners were asked to reveal whether the employees clicked on pop ups that appeared on the SME computers. The results were shown in Figure 4.7.

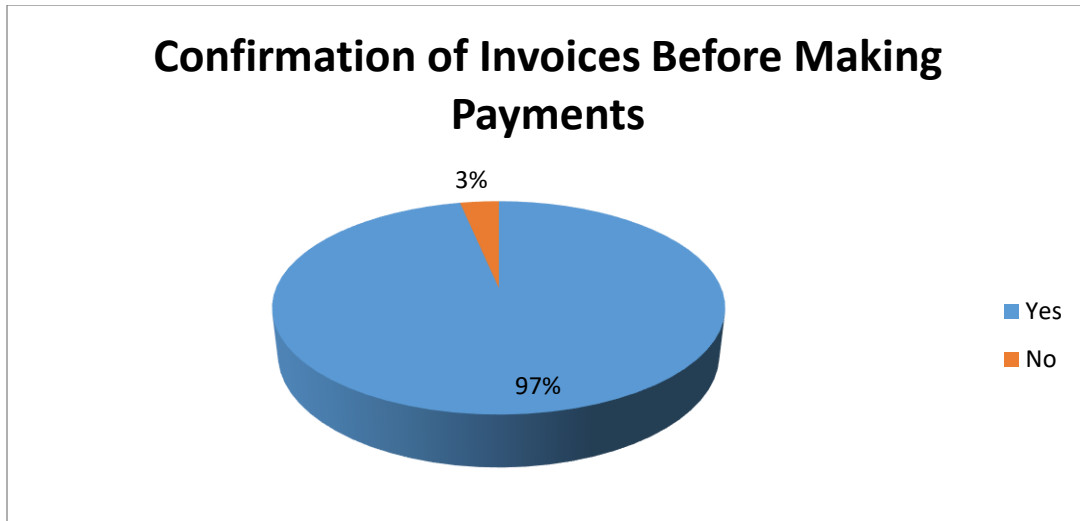


**Figure 4.7: Clicking of Pop-ups of SMEs' Computers** Source: Field Data (2023)

Data presented in Figure 4.7 showed that most of the SME owners (71%) revealed that the SMEs' employees did not click on pop-ups while using the business computers while a minority (29%) of the SME owners agreed that the SMEs employees clicked on pop-ups while using the business computers. Pop-ups are one of the tools used by cyber criminals engaged in phishing activities. Therefore, it is important that SME employees remain vigilant and avoid clicking on pop-ups while using not only the business electronic devices but also their personal electronic devices.

In a study by Iuga, Nurse, and Erola (2016) found that pop-up-related attacks had a noticeably greater success rate than other strategies, suggesting that consumers are more susceptible to these attacks. This conclusion is consistent with the findings of the present study, which show that only a small percentage of SME owners acknowledged situations in which staff clicked on pop-up windows. This implies that workers at SMEs generally exhibit a feeling of caution and understanding regarding the dangers posed by pop-ups. These results highlight the need of staff awareness in avoiding pop-ups to maintain effective cyber security safeguards.

The SME owners were further asked whether the SMEs employees confirm all the invoices before making any payments. The data collected is presented in Figure 4.8.



**Figure 4.8: Confirmation of Invoices Before Making Payments**

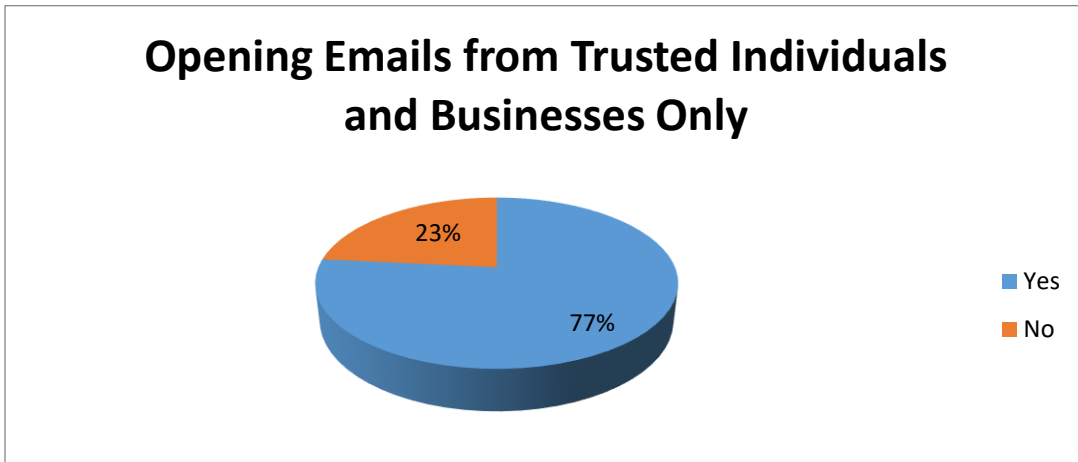
**Source: Field Data (2023)**

The results presented in Figure 4.8 showed that majority of the SME owners (97%) revealed that the SMEs employees were vigilant in making invoice confirmation before making any payments. This finding is essential since it showed that the SME owners are vigilant and understand that in the modern world it is easy to be conned using fraudulent invoices. Therefore, it is critical to ensure that the invoices presented to the SMEs either by a messenger or an individual purporting to be an employee must be confirmed to ensure payment is made to the right account. The SME owners argued that through the confirmation of the invoices, the SMEs have been able to make payments with referent to the correct amounts, dates and accounts.

This result was consistent with Chesimo's (2020) research, which focused on the negative impacts of fraudulent transactions on operational success, including the loss of potential sponsors, insolvency, failure to meet project objectives, and potential job losses for staff. SMEs can successfully reduce the danger of falling for scams or fraudulent transactions by

sticking to the practice of invoice verification before payment, so preserving their financial stability and maximizing operational effectiveness.

Further, the SME owners were asked whether the SMEs open emails from only the businesses and individuals they do business with or from everyone as long as it is directed to the business inbox. The findings were shown in Figure 4.9.



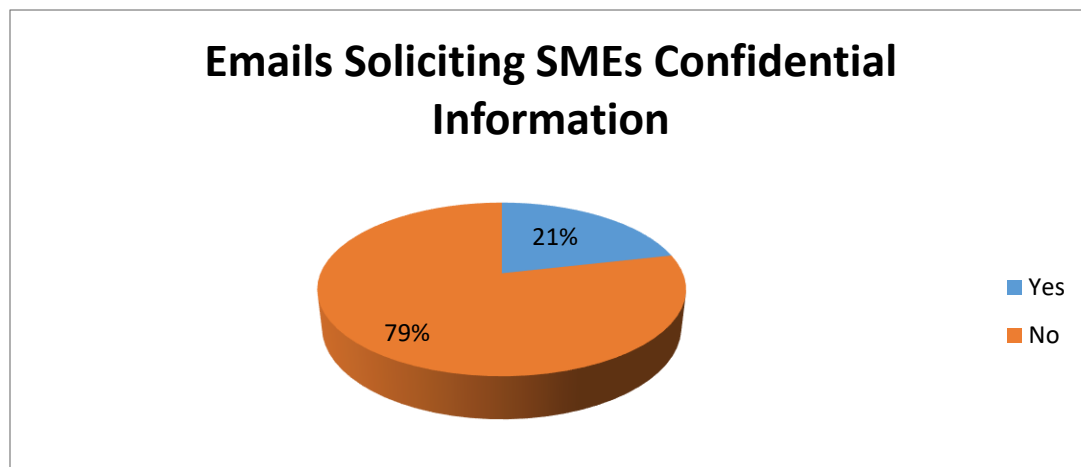
**Figure 4.9: Opening Emails from Trusted Individuals and Businesses Only**

**Source: Field Data (2023)**

Data presented in Figure 4.9 showed that 232 (77%) of the sampled SMEs employees only opened emails from trusted individuals and businesses. However, 71 (23%) of the sampled SMEs employees were identified to open emails from all individuals. Based on the findings, it was identified that the SMEs owners had directed the employees to only open the emails from trusted sources to avoid being victims of phishing. Nonetheless, as indicated by the 71 interviewees that reported opening all emails as long as they were directed to the business, there is need to educate the SMEs owners and employees on the importance of only opening emails from verified and trusted sources.

This finding was consistent with other research, such as that by Williams, Hinds, and Joinson (2018), who highlighted the need of warning SME owners and employees about the dangers of phishing scams and the need to confirm the legitimacy of receiving emails. These safety measures are essential for keeping SMEs safe from viruses or scams. The study's findings highlight how workplace routines and context affect how employees absorb information and react to questionable emails.

The researcher asked the SME owners to reveal whether the SMEs had received any emails soliciting confidential information about the business such as the account numbers and PIN numbers. The findings were shown in Figure 4.10.



**Figure 4.10: Emails Soliciting SMEs Confidential Information**  
**Source: Field Data (2023)**

Data presented in Figure 4.10 showed that a minority of the sampled SMEs (21%) had received emails soliciting the business confidential information. This is an indication that cyber criminals still attempt to phish their victims using emails. Notably, the SME owners revealed that while they had received emails soliciting the business confidential information, they did not reply to the emails. This is an indication that the SMEs owners

and employees understand the dangers of sharing confidential information about the business. This supports the idea that putting anti-phishing procedures into place and enforcing tight regulations for managing and securing personal information are essential to protecting SMEs from phishing attempts and maintaining their optimum performance. Esmat, Alharbi, and Karrar (2021) underline that enterprises must have effective anti-phishing procedures to maintain performance.

The qualitative data collected from the interviewees explained that the owners of the sampled SMEs did not understand the concept of phishing. However, one of the key informants said:

*“many owners of SMEs understand that they should not click on any pop-ups that they do not trust. However, they do not have an understanding of the concept of phishing and how it is used by cyber criminals”* (IT Specialist/Expert, 003)

Phishing was identified as a challenge for SMEs as posited by the IT specialist who added that the owners of SMEs were not deliberate in implementing cyber security strategies in their businesses. One of the interviewees explained that the SMEs owners only consulted IT specialists when they have already encountered a cybercrime. This according to the ICT specialist is a wrong time to bring in the experts since the damage has already been done. This finding is in accordance to results by Abroshan, Devos, Poels, and Laermans (2021) who observed that most SMEs only reach out to the IT specialists when an attack has already occurred.

With reference to the cyber-security strategies implemented by SMEs, the four ICT experts noted that most SMEs only have an anti-virus on their technological devices as the only measure against cybercrime. According to two of the IT experts/specialists, SMEs do not put in place necessary cyber-security measures. This was attributed to the fact that most SMEs do not use many computers and technological devices. However, one of the IT experts revealed that regardless of the size of the business, it is necessary for SMEs to put in place relevant cyber-security measures since more cyber criminals are emerging in the modern world of technology. This concurs with recommendations made by Nkurunziza, (2021) who established that cyber security is essential for any business irrespective of the size of the entity.

#### **4.4.4 Malware Attack**

The fourth objective of the study sought to determine the effect of malware attack on performance of SMEs based in Nairobi County, Kenya. Malware attack as described in the study is infecting a computer system with malicious software that can cause harm, such as stealing data, damaging files, or taking control of the system. Based on this definition, the SME owners were asked to reveal the individuals responsible for conducting updates on the SMEs electronic devices such as computers. The results were shown in Table 4.11.



**Table 4.10: Personnel Responsible for Conducting Updates on SMEs' Electronic Devices**

<b>Frequency</b>	<b>Frequency</b>	<b>Percentage</b>
IT personnel	82	27.1
Owner	123	40.6
Manager	65	21.5
Any Staff	33	10.8
<b>Total</b>	<b>303</b>	<b>100</b>

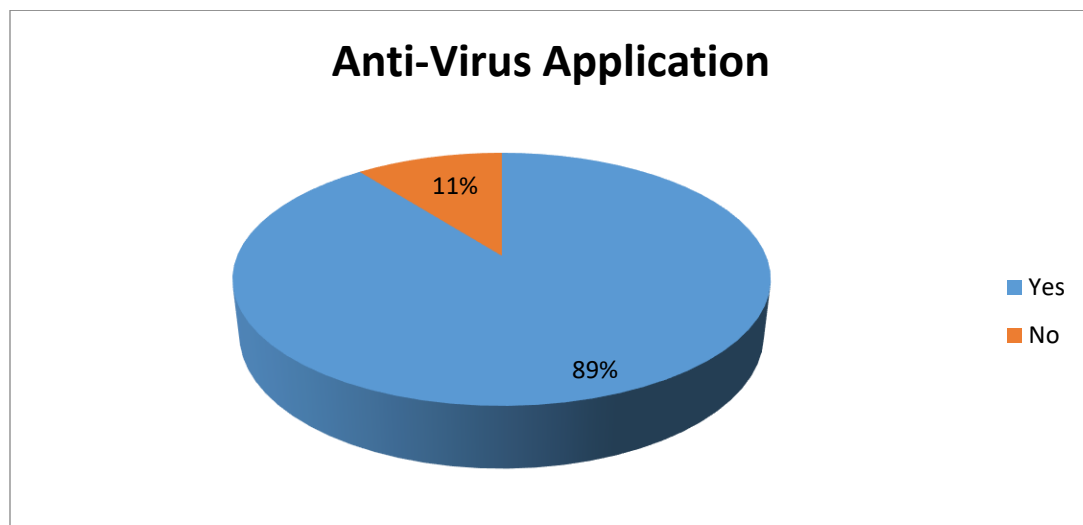
Source: Field Data (2023)

The findings in Table 4.11 showed that the personnel involved in conducting updates on the SMEs electronic devices is the owner (40.6%) followed by the IT personnel (27.1%) who is closely followed by the manager (21.5%). This was also observed by the researcher while conducting the research. The researcher observed the SMEs' owners making updates on the computer at the business entity. This finding was attributed to the fact that that SMEs are not large organizations that can afford to employ a full time IT team or employees. Notably, it is essential that SMEs make an extra effort in ensuring cyber security by ensuring that all the issues pertaining to their electronic devices are maintained and monitored by competent IT personnel. This will ensure that they remain vigilant to any malware attack or other forms of cybercrime.

Due to the size and budget constraints of SMEs, which frequently prevent the development of specialist IT departments, the study finds that SME owners are primarily responsible for updating their technological equipment. The results were consistent with Lévesque, Chiasson, Somayaji, and Fernandez's (2018) research, which showed that real-world

antivirus performance frequently performs worse than in controlled environments, and they emphasize the significance of qualified IT professionals in putting effective cyber security measures into place. Furthermore, their research revealed strong relationships between malware attacks and computer proficiency, network usage, and peer-to-peer behavior.

The SME owners were asked to indicate whether their electronic devices had an installed anti-virus application. The results were shown in Figure 4.11.



**Figure 4.11: Anti-Virus Application**

**Source: Field Data (2023)**

The data presented in Figure 4.11 showed that 89% of the sampled SMEs owners revealed that their electronic devices had an installed anti-virus application while 11% of them revealed they had not installed anti-virus application on their electronic devices. The findings revealed that the majority of the sampled SME owners had taken an initial step of protecting the business from any malware attacks by installing anti-virus application. The importance of the anti-virus application is that it protects the computer from any malware that may be sent via email, through pop-ups or by using external devices to share

information or make transfers such as the USB cable and flash disks. This is in line with Kumar, Ojha, and Srivastava, (2018) who established that the most important aspect of malware attacks is an inadequate software protection and that this factor is directly linked to costing components.

Further, the researcher enquired about the frequency in which the anti-virus application is updated in the SMEs. The findings were presented in Table 4.12.

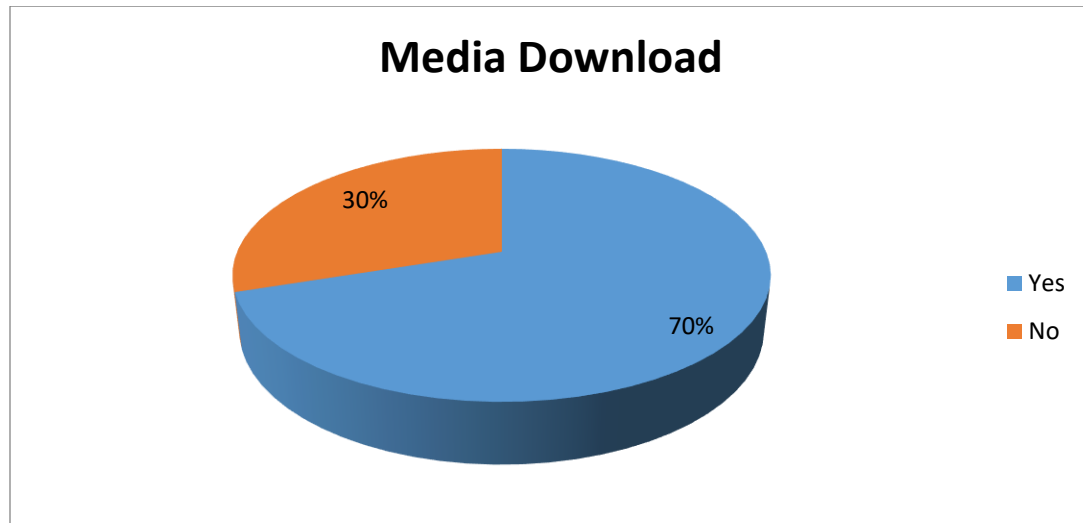
**Table 4.11: Frequency of Updating Anti-virus Applications**

<b>Frequency</b>	<b>Frequency</b>	<b>Percentage</b>
Daily	0	0
Weekly	0	0
Monthly	2	0.7
Annually	219	80.8
Never	50	18.5
<b>Total</b>	<b>271</b>	<b>100</b>

**Source: Field Data (2023)**

The findings shown in Table 4.12 show that 219 of the sampled SME owners updated their anti-virus application on an annual basis. Only 2 of the sampled SMEs updated their anti-virus application monthly. The findings also revealed that 50 of the SMEs never updated their anti-virus applications. The findings provide a justification for SMEs falling victim to cyber-attacks especially using malware attacks. This is because while the SMEs have installed the anti-virus application, they are not consistent in updating it, hence may not offer strong protection against malware attacks.

The SME owners were also asked to indicate whether the employees of the sampled SMEs download any media while using the business computer. The results were presented in Figure 4.12.



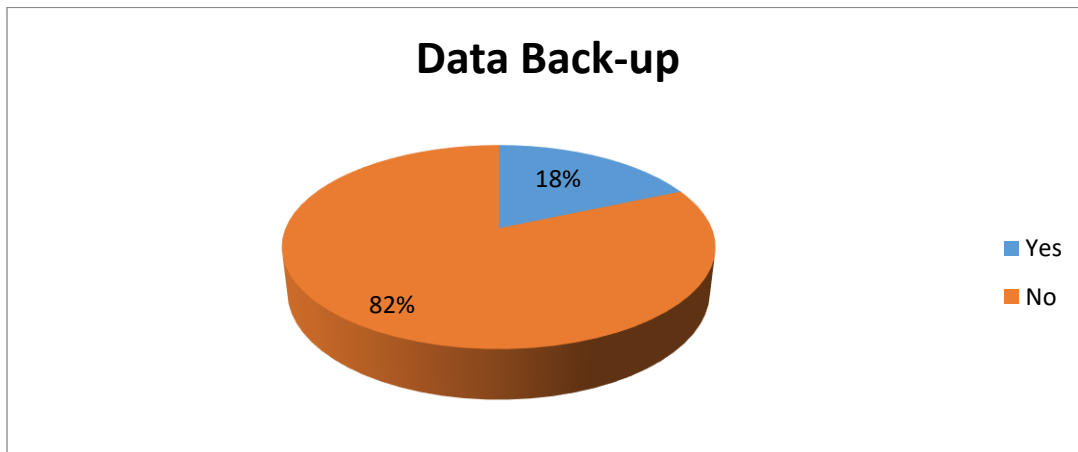
**Figure 4.12: Media Download**

**Source: Field Data (2023)**

The data presented in Figure 4.12 showed that 70% of the SME owners revealed that the employees from the SMEs downloaded media from the internet on the SME computer. This positions the SMEs at risk of downloading media with malware, hence making the business susceptible to malware attacks. The findings also show that 30% of the sampled SME owners indicated that the SMEs employees did not download media from the internet. This is a measure that protects the sampled SMEs from being victims of malware attacks. Silva's (2020) research affirms the challenges encountered in safeguarding networks due to the absence of dependable frequency monitoring and a comprehensive understanding of cyber-attack effects. This is consistent with the findings of the current study, which point to alarming patterns in SMEs' media download behaviors, data backup procedures, and

frequency of computer breakdowns brought on by malware attacks. As a result, taking proactive steps to reduce the likelihood of malware attacks and their negative effects on business operations and overall performance, such as finding vulnerabilities and conducting risk assessments, is crucial.

As indicated earlier, most of the sampled SMEs have a database with all the important information required for their day-to-day operations. With reference to this, the researcher sought to understand whether the SMEs had any data backup. The findings were shown in Figure 4.13 below.

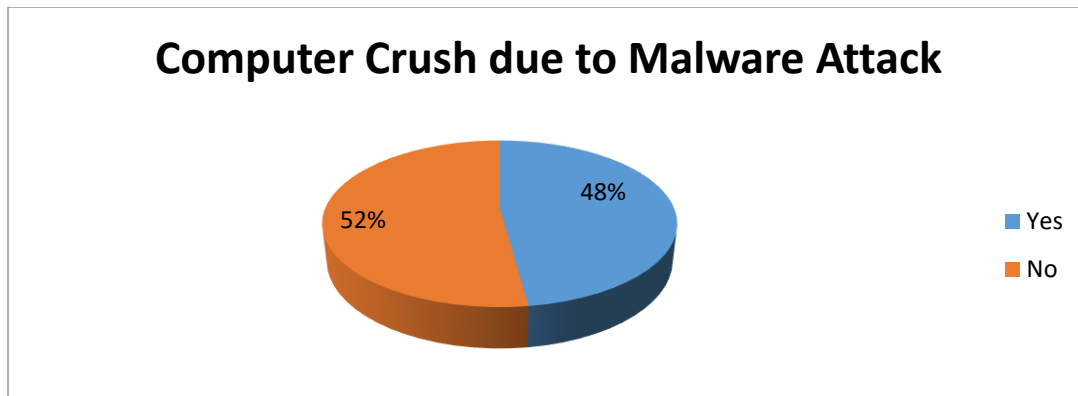


**Figure 4.13: Data Back-up**

**Source: Field Data (2023)**

The results presented in Figure 4.13 show that only 18% of the sampled SMEs had a data backup. Most of the sampled SMEs (82%) did not have a data back-up. This implies that in case of a malware attack, majority of the sampled SMEs would lose all their data.

The SME owners were asked whether the SME computer had ever crashed as a result of malware attacks. The findings were presented in Figure 4.14.



**Figure 4.14: Computer Crush due to Malware Attack** Source: Field Data (2023)

Figure 4.14 revealed that computers from 48% of the sampled SMEs had crashed as a result of the malware attack while 52% of the sampled SMEs' computers had not crashed as a result of malware attacks. The SME owners further revealed that following the computer crush, they sought the help of IT specialist who were able to retrieve the data saved and installed an anti-virus application. This finding showed the importance of engaging the assistance of IT specialists when dealing with computer issues.

The results of the research shed light on the potential consequences of malware attacks and data breaches on SMEs, including compromised consumer privacy, monetary risks, and negative performance effects. These results support Arunlal's (2019) analysis, which highlighted the significant loss of corporate data, intellectual property, brand reputation, and financial losses brought on by cyber-attacks. AlMarri's research from 2017 also underlines the use of anti-forensic tactics by malware and the limits in assessing these attacks owing to inferior technologies, resulting in ineffective outcomes and difficulties in acquiring trustworthy evidence. Although AlMarri's study does not specifically examine how malware assaults affect business performance, it does highlight the complexity and

severity of malware dangers and the need for strong cyber security measures to reduce their potential impact on business performance.

Data collected using the interview guide revealed that majority of the sampled SME owners did not understand the concept of malware attacks. According to two of the interviewees, the owners of SMEs understand malware attack as a virus that can be solved as long as the computer had an anti-virus. The interviewee noted that majority of the owners of SMEs were not vigilant in updating their anti-virus. This as posited by the interviewees, creates an opportunity for cyber criminals to use different malwares to access the SME's databases.

In addition, the IT specialist/experts indicate that a key challenge faced when working with SMEs is trying to convince them the importance of cyber-security. As noted earlier, the SMEs only call upon the IT specialist when the damage had been done. This poses a challenge since majority of the owners of SMEs do not believe that their businesses can be victims of cyber-crime as compared to larger organizations. One of the IT specialist added:

*“it is sad, that it takes so much energy and time to convince SMEs to implement cyber-security. This is because, today, many cyber criminals targeting larger corporations use SMEs as a conduit and as practice. Moreover, most cyber criminals already know that SMEs do not take deliberate actions to protect their business, hence can easily be targeted.”* (IT specialist/expert, 004)

Therefore, based on the above finding, the IT specialist explained that the best strategies that SMEs can implement to avoid being victims of cyber-crime is to bring in an IT specialist from the start. This is because, with the help of the IT specialist, a security system

can be developed based on the size of the businesses. Moreover, backups can be made to ensure that in case of any cyber-crime, the business information is not lost. One of the interviewees revealed that most SMEs do not like working with IT specialist since they deem it expensive, however the interviewee stated that the service of IT experts would be more expensive in the eventuality of a cyber-crime. Therefore, the interviewees emphasized on the importance of SMEs to collaborate with experts to ensure cyber security.

The results of the research show that the sampled SMEs frequently experience resource constraints that prevent them from investing in thorough cyber security measures, leaving them open to malware attacks. According to Kumar, Ojha, and Srivastava's (2018) results, insufficient software security emerges as the main cause of these attacks, with a connection to high-cost components. To stop these assaults and lessen their effect on the performance of SMEs, it is crucial to understand the importance of financial control and investment in malware security solutions.

#### **4.5 Performance of the SMEs**

The dependent variable of the study was performance which was measured using both financial and non-financial indicators. The indicators of financial performance were ROA and ROE from year 2017 - 2021. The findings were presented in Table 4.13.



**Table 4.12: Financial Performance of SMEs (2017-2021)**

	<b>N</b>	<b>Min</b>	<b>Max</b>	<b>Mean</b>	<b>Std Deviation</b>
ROA 2017	303	12.0	70.0	31.925	11.749
ROA 2018	303	12.0	70.0	30.978	11.820
ROA 2019	303	12.0	70.0	30.832	10.903
ROA 2020	303	9.0	62.0	28.637	10.637
ROA 2021	303	9.30	62.0	28.933	10.563
ROE 2017	303	2.0	27.0	11.110	4.2684
ROE 2018	303	2.0	25.0	11.297	5.8263
ROE 2019	303	2.0	27.0	11.639	4.2739
ROE 2020	303	2.0	22.0	11.314	4.8263
ROE 2021	303	2.0	22.0	11.093	4.7282

**Source: Field Data (2023)**

The highest Return on Asset (ROA) for the sampled SMEs throughout the aforementioned time, as shown in Table 4.13, was 70%, demonstrating a respectable ability to create profits relative to their asset base. In contrast, the SMEs' minimum ROA was 9%, which suggests either lower profitability or correspondingly less effective utilization of assets. The wide range of financial performance among the sampled SMEs in the Kamukunji constituency is indicated by the significant variance in ROA, as indicated by the high standard deviation ranging from 10 to 11. Additionally, over the indicated time period, the average ROA mean showed a dropping tendency, decreasing from 31.925 to 28.637. This dip denotes a slowing of the constituency's small business sector's rate of expansion. This may be attributed to the Covid-19 pandemic that affected all businesses around the world.

Turning to the Return on Equity (ROE), the data from 2017 to 2021 revealed that the sampled SMEs in the Kamukunji constituency performed only moderately well. The average ROE for these businesses ranged from 11.093 to 11.639, which showed a consistent but moderate ROE. The highest ROE recorded throughout the period was 27%, highlighting a rather successful use of equity. Contrarily, for the entire period from 2017 to 2021, the minimal ROE was consistently at a low level of 2%. This persistent and modest minimum ROE clearly showed that SMEs in the Kamukunji constituency consistently perform below average in terms of their ROE.

Additionally, performance was measured using non-financial indicators. Using a five-point Likert scale, the SME owners were asked to show their level of agreement on non-financial statements. The findings were presented in Table 4.14.

**Table 4.13: Non –Financial Performance**

<b>Statements</b>	<b>Mean</b>	<b>Std Deviation</b>
i. The customer base of the SME has increased	3.83	1.190
ii. The SME has launched new products and services	3.87	1.283
iii. The SME has gained a loyal customer base	4.02	0.853
iv. The SME has expanded its operations to other geographical areas	3.43	1.027
v. The SME has received good feedback from its customers	4.21	0.734
vi. The SME’s employee turnover has decreased	3.87	1.284
<b>Average</b>	<b>3.87</b>	

**Source: Field Data (2023)**

The SME owners to a moderate extent agreed with the statements on non-financial statements as recorded a mean of 3.87. The highest ranked statement was that the sampled

SME had received good feedback from its customers: With a mean score of 4.21, the findings indicate that SMEs have generally received positive feedback from their customers. The low standard deviation of 0.734 suggests a consistent pattern of favorable customer feedback across different SMEs. This finding suggests that the SMEs samples, on average, have effectively met customer expectations and received positive reviews, which can contribute to their reputation and success.

The SME owners agreed that the SME had gained a loyal customer base (Mean = 4.02; Standard deviation = 0.853) This finding suggests that SMEs, on average, have been effective in fostering customer loyalty, which can be indicative of customer satisfaction and repeat business. The mean score of 3.83 suggests a moderate increase in the customer base of SMEs. This finding implies that most of the sampled SMEs experienced growth in their customer base, although the magnitude of this growth may vary.

The statement on launching new products and services scored a mean score of 3.87 and suggesting that while many SMEs have engaged in introducing new products/services, the degree of innovation and diversification varies across them. The SME owners also moderately agreed to the statements on decreased employee turnover (Mean = 3.87; standard deviation = 1.284) and the sampled SME had expanded its operations to other geographical areas (Mean = 3.43; standard deviation = 1.027). The findings show that the non-financial performance of the sampled SMEs differed from one business to the other as exhibited by the moderate mean scores recorded.

#### **4.6 Regression Analysis**

To determine how the research variables interacted with one another, a linear regression analysis was conducted. This analytical approach aimed to assess the relationships between

cybercrime and SME performance in Kenya's Kamukunji constituency. The linear regression analysis made it easier to determine the coefficients associated with the variables under study. These coefficients were crucial in figuring out how much fluctuation in the independent variable, cybercrime, accounted for variance in the dependent variable, SMEs' performance. In Table 4.15, the model summary is displayed.

**Table 4.14: Model Summary**

<b>Model</b>	<b>R</b>	<b>R Square</b>	<b>Adjusted Square</b>	<b>R Std. Error of the Estimate</b>
1	0.8993	0.80874	0.794028	0.270996

Source: Field Data, 2023

Table 4.15 showed that the coefficient of determination ( $R^2$ ) was calculated to be 0.808, meaning that approximately 80.8% of the variation in the performance of SMEs in Kamukunji constituency can be attributed to the independent influences of cybercrime. It should be noted, however, that 19.2% of the performance variations remain unexplained, suggesting that there may be additional factors that were not included in this study.

To establish the overall statistical significance of the regression model, an analysis of variance (ANOVA) was performed as the next stage in the regression analysis. The ANOVA findings are displayed in Table 4.16, which provides crucial information about how well the regression model typically accounts for the observed difference in performance of SMEs.

**Table 4.15: ANOVA**

<b>Model</b>		<b>Sum of Squares</b>	<b>Df</b>	<b>Mean Square</b>	<b>F</b>	<b>Sig.</b>
1	Regression	12.732	1	4.244	55.111	0.004
	Residual	3.011	301	0.077		
	Total	15.743	302			

**Source: Research, (2023)**

Table 4.16 showed a significant correlation between the predictor variables and the dependent variable, as shown by the obtained significance value of 0.004 being smaller than the preset significance level of 0.05. Additionally, it was established that the essential F value at a 5% level of significance is 3.84. The model's statistical importance for the research was highlighted by the fact that the calculated F value (55.111) was higher than the F value. Furthermore, the linkages in the study model were examined using the coefficient table.

**Table 4.16: Coefficient of Determination**

<b>Model</b>		<b>Unstandardized Coefficients</b>		<b>Standardized Coefficients</b>		<b>Sig.</b>
		<b>B</b>	<b>Std. Error</b>	<b>Beta</b>	<b>t</b>	
1	(Constant)	0.289	1.2187		1.615	0.216
	Cyber-crime	-0.708	0.1523	0.178	4.219	.0186

Source: Field Data, (2023)

The relationship between the independent and dependent variables was demonstrated using a linear regression analysis. The following equation was generated based on the SPSS results from Table 4.17:

$$Y = \beta_0 + \beta_1 X_1 + \varepsilon$$

$$Y = 1.144 - 0.708 + \varepsilon$$

According to the findings of the linear regression study, cybercrime, an independent variable, had an effect on the performance of SMEs in Kenya's Kamukunji constituency. Keeping all other factors constant, the regression coefficient for the performance of SMEs was determined to be 0.289. Additionally, the research showed that a one-unit increase in cyber-crime was linked to a 0.708 decrease in performance of SMEs in Kamukunji constituency, Kenya.

The performance of the sampled SMEs is negatively impacted by cybercrime, according to the study's regression analysis. This conclusion supports the descriptive findings, which show that cybercrime in SMEs have a negative impact on performance because they cause the loss of client relationships. Additionally, the results were consistent with those of Janakiraman, Lim, and Rishika (2018), who showed that cybercrime cause large drops in consumer spending, which have a detrimental effect on performance.

## **CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS**

### **5.1 Introduction**

This chapter encapsulates the research findings and delineates the conclusions derived from them. Additionally, it encompasses recommendations and suggestions for future research.

### **5.2 Summary of the Findings**

The study assessed the effect that data breaches have on the performance of SMEs in Nairobi County, Kenya. According to the findings, data breaches have a negative impact on the performance of SMEs in Nairobi County, Kenya. The findings of this study demonstrate the value of customer data in SME databases and the necessity for SMEs to comprehend and satisfy consumers' expectations. The results revealed that 68% of the sampled SMEs had experienced data breaches. This raises concern over the compromised consumer privacy and financial concerns that might harm SME performance. Therefore, it is crucial for SMEs to establish robust cyber security measures to safeguard their databases and lessen any unfavorable performance repercussions. Moreover, the findings indicate that SME owners (50.8%) and managers (40.6%) frequently access databases, giving them knowledge of daily operations within the SMEs.

Secondly, the impact of identity theft on performance of SMEs based in Nairobi County, Kenya was evaluated. The study established that identity theft has a negative effect on the performance of SMEs in Nairobi Kenya. The study established that According to the study's findings, SME managers (37.3%) and owners (61.1%) often have the most access to contact lists, which is in line with the hierarchical structure that is frequently present in SMEs. IT staff (1.6%), on the other hand, had restricted access and prioritizes contact

management over cyber security. The study also established that the important safeguards against identity theft include creating policies that forbid unauthorized data transfers (100% of the SME owners agreed) and limiting access to particular data within an organization. Prioritizing regular password updates and stringent rules would help to solve the vulnerabilities brought on by negligent password management. The study's findings are consistent with the Routine Activity Theory, which contends that criminal activity, including cybercrime, requires a motivated offender, a lack of security, and a suitable victim. As a result, it is wise to restrict access to sensitive information in SMEs to just those who need it, such as client contact information and personal data.

Thirdly, the study evaluated how phishing influenced SMEs' performance in Nairobi County, Kenya. The results indicated that phishing negatively impacts on the performance of SMEs in Nairobi County, Kenya. The results of the study show that the sampled SMEs employees were cautious about clicking on pop-ups using the work-place computers (71%). Moreover, the results revealed that SMEs place a high priority on the practice of verifying invoices before making payments (97%). SMEs can lessen their vulnerability to fraud and maintain financial stability by following invoice verification procedures. The study also showed that the sampled SMEs were often cautious when receiving emails that ask for sensitive company information (77%), underscoring the importance of putting anti-phishing protocols in place and enforcing stringent rules to safeguard SMEs from phishing efforts and improve performance.

The fourth objective looked at how malware attacks impacted on SME performance in Nairobi County. The study established that malware attack negatively influences the performance of SMEs in Nairobi County, Kenya. The findings showed that while 89% of



the SME owners indicated that they had installed an antivirus on the work computers, only 0.7% revealed to having updated their antivirus on a monthly basis. The majority, 80.8% of the SME owners revealed that the antivirus on the workplace computer is updated annually. The main source of malware was identified to be media download (70%). This finding emphasizes the importance of being cautious when downloading any form of media from the internet. The findings from the regression analysis indicated that cybercrime (measured by data breach, phishing, identity theft and malware attack) has a negative and significant effect on the performance of SMEs in Nairobi County, Kenya.

### **5.3 Conclusions**

Cybercrime is a pervasive global problem that presents significant challenges for businesses worldwide. SMEs are in a particularly difficult situation when it comes to fighting cybercrime since they have fewer resources and are less able to put in place comprehensive preventive measures than larger organizations. The results of the study show that cybercrimes (data breaches, identity theft, phishing, and malware attacks), have a negative impact on the performance of SMEs. Customers' trust is particularly undermined by data breaches since their personal information becomes a top target for cybercriminals, which results in customer churn and decreased loyalty. Identity theft intensifies the negative effects on SME performance by associating the business with criminals, which could result in lost business and client trust. Furthermore, malware and phishing attacks degrade performance by having the potential to result in financial losses due to fraudulent activity. In order to properly address and avoid cyber dangers, SMEs must devote enough financial resources. SMEs can boost their performance while also ensuring their long-term viability in the face of rising cyber hazards by investing in strong cyber-security measures.

#### **5.4 Recommendations of the Study**

In light of the conclusions drawn from the specific objectives, this study recommends that SMEs should prioritize putting in place strong cyber security measures to protect their databases from potential cybercriminals. This can be done by limiting unauthorized data transfers and access, updating passwords frequently, and enforcing strict rules to effectively mitigate the risks associated with identity theft resulting from careless password management. Additionally, encouraging staff awareness and care becomes essential in successfully thwarting phishing assaults, especially those connected to pop-ups, while concurrently enforcing anti-phishing standards and stringent rules that can offer the required safeguards.

The study also recommends that SMEs can gain from collaborating with outside cyber security experts or consultants who focus on aiding companies protect their digital assets. These experts may carry out thorough security evaluations, provide specific recommendations, and give continuing assistance with putting in place efficient security measures. SME's can gain access to the most recent information and skills in cyber security by working with specialists in the industry.

The study recommends that the employees in SMEs should be vigilant in verifying the details of all the customers making electronic and plastic payments. This helps in identifying cases of identity theft. This should be embedded in all SME employees to ensure that the SMEs do not fall victim to the actions of cyber criminals.

The study recommends that SMEs should have a clear incident response strategy in place to deal with possible security incidents right away. This strategy should specify the actions to be performed in the event of a cyber-security incident, such as a malware attack or data

breach. It should outline steps for containing the issue, looking into its root cause, alerting the appropriate parties, and getting things back to normal. SMEs may lessen the effects of security events and cut downtime by having a written and tested incident response plan.

### **5.5 Suggestions for Further Studies**

The study focused on cyber-crime from a perspective of SMEs. While SMEs fall victim to cyber-crime, further studies should be conducted targeting larger organizations. Moreover, the study sets a foundation for further research to be conducted focusing on cyber-security strategies that can be put in place by SMEs to avoid being victims of cyber criminals. The study was based in Kamukunji, constituency in Nairobi County. Therefore, this study suggests that further research should be conducted in other counties to provide a framework to make comparisons of the cyber-crimes committed against SMEs in different counties.

## REFERENCES

- Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9, 44928-44949.
- Alahmari, A., & Duncan, B. (2020, June). Cyber security risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-5). IEEE.
- Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cyber security risks for mitigating data breaches in business systems. *Applied Sciences*, 11(8), 3678.
- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3, 563060.
- AlMarri, S. (2017). *A structured approach to malware detection and analysis in digital forensics investigation*. Thesis, [University of Bedfordshire](#).
- Almatrooshi, B., Singh, S. K., & Farouk, S. (2016). Determinants of organizational performance: a proposed framework. *International Journal of Productivity and Performance Management*, 65(6), 844-859.
- Apau, R., & Koranteng, F. N. (2019). Impact of Cybercrime and Trust on the Use of E-Commerce Technologies: An Application of the Theory of Planned Behavior. *International Journal of Cyber Criminology*, 13(2).

- Arunlal, K.S. (2019). Impact of Malware in Modern Society. *Journal of Scientific Research and Development*, 2, 593-600.
- Azadegan, A., Mellat Parast, M., Lucianetti, L., Nishant, R., & Blackhurst, J. (2020). Supply chain disruptions and business continuity. *Decision Sciences*, 51(1), 38-73.
- Bendle, M. N. (2019). Cyber Crimes: A Challenge to E-Commerce. *Our Heritage*, 68(9), 358-364.
- Benedict, A., Gitonga, J. K., Agyeman, A. S., & Kyei, B. T. (2021). Financial determinants of SMEs performance. Evidence from Kenya leather industry. *Small Business International Review*, 5(2), e389.
- Berger, Y. G., & De La Riva Torres, O. (2016). Empirical likelihood confidence intervals for complex sampling designs Series B Statistical methodology. *Journal of the Royal Statistical Society* 78(2), 319-341
- Boateng, R., Olumide, L., Isabalija, R.S. & Budu, J. (2011). Sakawa: Cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, 11(2), 85–100.
- Böhme, R., & Moore, T. (2012, October). How do consumers react to cybercrime?. In *2012 eCrime researchers summit* (pp. 1-12). IEEE.
- Bryman, A. (2011). Research methods in the study of leadership. *The SAGE handbook of leadership*, 15-28.
- Chesimo, C. C. (2020). *Influence of fraud on operational performance in non-governmental organizations within Nairobi County* (Doctoral dissertation, Strathmore University).
- Clarke, R. V., & Felson, M. (1993). *Routine activity and rational choice*. New Brunswick, NJ: Transaction Publishers.

- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588-608
- DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, 5(4), igab043.
- Esmat, H. Y., Alharbi, A. F., & Karrar, A. (2021). The Impact of Phishing on the Business Sector in KSA: Analytical Study. *International Journal*, 10(2).
- Gadirova, N. (2021). *The Impacts of Cyberattacks on Private Firms' Cash Holdings* (Doctoral dissertation, Université d'Ottawa/University of Ottawa).
- Githuku, D. N. (2019). *Relationship Between Loan Amount Accessed And Growth Of Small And Medium Size Enterprises In Nairobi City County* (Doctoral dissertation, UoN).
- Gundu, T. (2019, February). Acknowledging and reducing the knowing and doing gap in employee cyber security compliance. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security* (pp. 94-102).
- Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6(1), 1-20.
- Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82(2), 85-105.
- Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*.
- Knight, S. (2020). *Strategies to Reduce Small Business Data Security Breaches* (Doctoral dissertation, Walden University).

- Kumar, A., Ojha, N., & Srivastava, N. K. (2018). Factors Affecting Malware Attacks: An Empirical Analysis. *PURUSHARTHA-A journal of Management, Ethics and Spirituality*, 10(2), 46-59.
- Laudon, K. C., & Traver, C. G. (2016). *E-commerce: business, technology, society*. 12th Edition, Pearson Education. Edinburgh. United Kingdom (UK)
- Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and human factors of malware attacks: A computer security clinical trial approach. *ACM Transactions on Privacy and Security (TOPS)*, 21(4), 1-30.
- Mohammed, Z. (2021). Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. *Organizational Cyber security Journal: Practice, Process and People*.
- Mugenda, O.M. & Mugenda, A.G. (2003) *Research Methods, Quantitative and Qualitative Approaches*. ACT, Nairobi.
- Mustaine, E. E., & Tewksbury, R. (1998). Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures. *Criminology*, 36, 829-857.
- Mwai, M. N. (2015). *Factors Contributing To Occurrence Of Cybercrime On E-Banking In Commercial Banks In Kenya* (Doctoral dissertation, United States International University-Africa).
- Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The rapid growth of cybercrimes affecting information systems in the global: is this a myth or reality in Tanzania?. *International Journal of Information Security Science*, 3(2), 182-199.

- Nkurunziza, A. S. (2021). *A Framework for Cyber security Risk Management: A Case of ICT SMEs in Nairobi, Kenya* (Doctoral dissertation, United States International University-Africa).
- Okeke, R. I. (2015). *The prevention of internal identity theft-related crimes: a case study research of the UK online retail companies* (Doctoral dissertation, University of Central Lancashire).
- Olonde, N. (2017). Entrepreneurs and entrepreneurship in Africa: What is known and what needs to be done. *Journal of Developmental Entrepreneurship*, 7(3)
- Ouma, C. (2021). *Effective Cyber Incident Response Capability Framework for County Governments in Kenya: a Case of Migori County* (Doctoral dissertation, University of Nairobi).
- Patel P., Patel, R., Patel, V. & Pathrabe, T. (2017). Survey of Privacy and security issues in spice world e-commerce website. *International Journal for Innovative Research in Science & Technology*, 19-23.
- Piquero, N. L., Piquero, A. R., Gies, S., Green, B., Bobnis, A., & Velasquez, E. (2021). Preventing identity theft: perspectives on technological solutions from industry insiders. *Victims & offenders*, 16(3), 444-463.
- Rakololo, W. M., & Maluleke, W. (2020). An Exploratory Study on Causes of Identity Document Theft in South Africa. *International Journal of Criminology and Sociology*, 9, 670-685.
- Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?. *International Review of Law, Computers & Technology*, 35(2), 131-161.



- Rofiq, A. (2012). *Impact of cyber fraud and trust of e-commerce system on purchasing intentions: Analysing planned behaviour in Indonesian business* (Doctoral dissertation, University of Southern Queensland).
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.
- Silva, N. (2020). *Malware Attacks affecting organizations*. (Project, Florida Institute of Technology).
- Twisdale, J. A. (2018). *Exploring SME Vulnerabilities to Cyber-criminal Activities Through Employee Behavior and Internet Access* (Doctoral dissertation, Walden University).
- Vanhee, A. (2020). *The Impact Of Identity Theft Victimization On The Use Of Protective Measures*. Thesis, The Pennsylvania State University.
- Warner, J. (2011). Understanding Cyber-Crime in Ghana: A View from Below. *International Journal of Cyber Criminology*, 5(1), 736–749.
- Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, 5(1).
- Wekundah, R. N. (2015). *The effects of cyber-crime on e-commerce; a model for SMEs in Kenya* (Doctoral dissertation, University of Nairobi).
- Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1-13.
- Yucedal, B. (2010). *Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories* (Doctoral dissertation, Kent State University).

## APPENDICES

### APPENDIX I: QUESTIONNAIRE FOR SME'S BUSINESS OWNERS

The goal of this study tool is to collect information about the impact of cybercrime on the performance of SMEs in Nairobi County, Kenya. Please follow the directions provided when completing the questionnaire. You can be confident that any information you share will be kept private. Furthermore, the information you provide will only be used for academic purposes. Please do not provide any personal information in this questionnaire, such as your name or identification number.

#### SECTION A: DEMOGRAPHIC INFORMATION

1. Kindly indicate your gender.

Male [ ]                      Female [ ]

2. Kindly indicate your age bracket.

Below 20 years [ ]

21-30 years [ ]

31-40 years [ ]

41-50 years [ ]

Above 50 years [ ]

3. Kindly indicate your highest level of education.

No formal education [ ]

Primary level [ ]

Secondary level [ ]

College level [ ]

University level [ ]

Postgraduate level [ ]

4. How long have you operated the SME?

Below 1 year [ ]

1-5 years [ ]

6-10 years [ ]

11-15 years [ ]

16-20 years [ ]

Above 20 years [ ]

5. Which information technology (IT) does the SME use? Tick where appropriate

Telephone and radio equipment [ ]

Software [ ]

Personal computers [ ]

Office Computers [ ]

Cell phones [ ]

Computer Applications [ ]

Audio and visual technology [ ]

Internet [ ]

Printer [ ]

Photocopy machine [ ]

Other.....

6. How often do you use information technology (IT) to run the SME?

Daily [ ]

Weekly [ ]

Not at all [ ]

**SECTION B**

**(a) Data Breach**

7. Does the SME have an SME database?

Yes [ ]

No [ ]

8. What type of information is saved on the SME database if the answer is yes in question 7 above?

Customer's information [ ]

Suppliers' information [ ]

Customer orders [ ]

Customer purchases [ ]

Daily sales [ ]

Transactions made [ ]

Other.....

9. Who has access to the SME database?

SME owner [ ]

Manager [ ]

IT personnel [ ]

Other.....

10. Has the SME ever had a data breach (a situation in which information is stolen from a computer without the owner's knowledge or consent)?

Yes [ ]

No

If yes, explain how? .....

11. If your answer to question 10 was yes, what type of data was stolen without the knowledge or authorization of the SME system owner?

Client's contact

Financial records

Supplier's contacts

Investor's contact

The SME inventory

Other.....

**(b) Identity Theft**

12. Who can access the contact list of all of the SME customers and suppliers?

Owner

Management

Supervisors

Other.....

13. Are the SME employees allowed to copy any data from the SME computer devices to their personal information technology devices?

Yes

No

If yes, which type of data are they allowed to copy from the SME computer?.....

14. Does the SME electronic devices have passwords?

Yes [ ]

No [ ]

15. If yes to the above question, how often is the SME password changed?

Daily [ ]

Weekly [ ]

Monthly [ ]

Never [ ]

16. Does the SME staff require to see the identification of all customers paying through electronic money transfer?

Yes [ ]

No [ ]

17. Does the SME staff require to see the identification of all customers paying with debit or with credit cards?

Yes [ ]

No [ ]

18. Has the SME experienced identity theft (the fraudulent practice of using another person's name and personal information to obtain loans or purchase of goods/services)?

Yes [ ]

No [ ]

If yes, kindly indicate how.....

**(c) Phishing**

19. Do the employees click on pop-ups while using the SME computers or devices?

Yes [ ]

No [ ]

20. Do the employees in the SME confirm details about invoices before making any payments?

Yes [ ]

No [ ]

If yes, how has this been helpful to the SME? .....

21. Does the SME management instruct the employees only to open emails from the people they do business with only?

Yes [ ]

No [ ]

If yes, how has this practice helped in protecting the SME? .....

22. Do the employees send personal emails or reply to personal emails using the SME computer?

Yes [ ]

No [ ]

If no, explain why.....

23. Has any of the employees in the SME ever received an email soliciting (requesting) for confidential information about the SME business?

Yes [ ]

No [ ]

If yes, explain what happened.....

**(d) Malware Attack**

24. Who conducts updates for the SME computers/devices?

IT professional [ ]

Owner [ ]

Managers [ ]

Any staff [ ]

Other.....

25. Do all SME computers have an anti-virus application?

Yes [ ]

No [ ]

If yes, indicate the anti-virus application installed in the SME computers?.....

26. How often are the computer antivirus updates done in the SME?

Daily [ ]

Weekly [ ]

Monthly [ ]

Annually [ ]

Never [ ]

27. Do employees download anything from the internet while using SME computers?

Yes [ ]

No [ ]

28. Does the SME have a data backup?

Yes [ ]

No [ ]



29. Has any of the SME's computers ever been crushed due to a malware attack (this is a malicious software that performs unauthorized functions on a victims computer system?)

Yes [ ]

No [ ]

If yes, how was the situation handled.....

**SECTION C: FIRM PERFORMANCE**

**a) Financial Performance**

Indicate the return on equity in the SME for the last 5 years in the table below

Indicator	2017	2018	2019	2020	2021
Return on Equity(All Assets minus Liabilities)					

Indicate the return on asset in the SME for the last 5 years in the table below

Indicator	2017	2018	2019	2020	2021
Return on Asset (Net Income ÷ Total Assets)					

**b) Non-financial Performance**

To what extent do you agree or disagree with the following statements on the non-financial performance of SMEs within Nairobi County for the last five years? Rate on a scale of 1 to 5 where 1= strongly disagrees, 2= disagree, 3= undecided, 4= agree and 5 strongly agree

Description and characteristics	1	2	3	4	5
vii. The customer base of the SME has increased					
viii. The SME has launched new products and services					
ix. The SME has gained a loyal customer base					
x. The SME has expanded its operations to other geographical areas					
xi. The SME has received good feedback from its customers					
xii. The SME's employee turnover has decreased					

**“THANK YOU FOR YOUR PARTICIPATION”**

## **APPENDIX II: KEY INFORMANT INTERVIEW GUIDE**

My name is Jacinta Nduku Mulei a University of Nairobi Post-graduate student. I am carrying out research on the effect of cybercrime on performance of SMEs in Nairobi County, Kenya. Any information you share will be used in confidentiality. Your personal information will not be disclosed.

1. In your opinion, which cybercrimes are common in SMEs?
2. In your opinion, do the SMEs' owners and employees understand the following concepts; phishing, data breach, identity theft and malware attacks?
3. Who are the common perpetrators of cybercrime in SMEs in your opinion?
4. What is your opinion on the cyber security measures used by SMEs?
5. In your opinion, do SMEs consider cyber security essential for the day-to-day operations of a business?
6. Based on the SME's you have worked with, which is the largest challenge faced by SMEs while trying to implement cyber security measures?
7. Based on your experience as an IT expert, which is the common end goal for individuals committing cybercrime against SMEs?
8. Is it possible for SMEs to recover all of their information in the event of the occurrence of cybercrime?
9. Which are the best strategies that SMEs can implement to protect their businesses?

**“THANK YOU FOR YOUR TIME”**