-

A CASE STUDY ON THE IMPACT OF CYBERSECURITY ON SMALL MEDIUM ENTERPRISES IN NAIROBI COUNTY DURING COVID-19 PERIOD.

By

Melchizedek Gichure Mwangi

19ZAD103890

Supervisor: Mr. David Kirop

A RESEARCH PROJECT SUBMITTED IN FULFILLMENT FOR AWARD OF DIPLOMA IN BUSINESS INFORMATION TECHNOLOGY IN THE RIARA BUSNIESS SCHOOL.

JUNE 2021

DECLARATION

This project proposal is my genuine original work and has not been

Submitted to this and any other institution.

Signature:

Date: May 2021

Name: Melchizedek Gichure

Admission Number: 19AD103890

APPROVAL

This project proposal has been supervised and approved by me as the university supervisor.

Signature: …........................

Date: …................................

Name: …..............................

Lecturer: Mr. David Kirop

DEDICATION

I hereby dedicate this project to the Lord Almighty, the pillar of my strength to guide me through it and give me the right mind state to

work on it till completion. Also to my parents for always being there to advise me righteously in all my years of education.

ACKNOWLEDGEMENT

I am grateful to the Lord for guiding me this far through my journey in education and also giving me an opportunity each and other day to make myself better. I am also grateful for my parents for believing in me and for the immense support. My friends to for supporting me. Finally, to my supervisor who tirelessly advised me and giving me morale when I was about to give up, Thank you all.

Table of Contents

ABSTRACT

This research proposal aims at discovering how cyber security has affected SME's. Living in such a dynamic society, businesses need to stay updated every day on emerging technologies and to suit customer demands. This has led to dependence of organizations on internet and Information Technologies. A liability is that it has led to development of cybercrimes. Cybercrime has been neglected in our society as not being a major concern. This study aims at conducting an empirical study by exploring, surveying and analyzing SME's around Nairobi on their practices on security.

ABBREVIATIONS

Abbreviation	**Description**
BYOD	Bring your own Device
IOT	Internet of Things
MSE	Micro and Small Enterprises
MSME	Micro Small and Medium sized Enterprise
ND	Not Defined
PC	Personal computer
RAT’s	Remote Access Tools
SME	Small Medium Enterprises
SMBs	Small-to-Mid-sized business
UN	United Nations
WTO	World Trade Organization

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND OF STUDY

SME’s are small medium enterprises that maintain incomes, resources or various workers under a specific edge (Ward, 2020.) Although the small medium enterprises are small in size they play an important role in the economy by outnumbering large firms significantly, utilize immense quantities of individuals and are for the most part pioneering in nature, assisting with forming advancement. Small medium enterprises have proven to be pillars in the growth of the society, but during the pandemic they were hit hard and the government had to get involved to save them from falling deep into debt. The Cabinet Secretary for National Treasury and Planning, Amb. Ukur Yatani stated in order to de-risk lending Micro, Small and Medium Enterprises he had set aside Sh 3 billion seed capital to operationalize the Credit Guarantee Scheme. The Credit Guarantee Scheme will enable the issuance of affordable credit in an efficient and structured manner in a recovery bid for the sector. Kenya thrives on the wheels of Small medium enterprises currently estimated to be contributing at least 45% to Kenya’s Gross Domestic Product and contributes 86% to employment opportunities. **ND (2020.)**

1.2 PROBLEM STATEMENT

When the pandemic occurred, it forced to change how we live our day-to-day lives from learning to working and how interact with each other. The pandemic proved to be a health crisis, which has affected the economy drastically. (Tuzo Jonathan,2021). SME proprietors have encountered dramatic falls in business movement and income because of limitations emerging from the pandemic, and are battling to pay their representatives and stay above water. (Coco D,2020). Effects of lockdowns have cause large and small business to collapse. Due to restrictions set up by the Ministry of Health and WHO, SME’s owners have experienced dramatic falls in business action and income because of limitations emerging from the pandemic, and are battling to pay their employees and stay above water.

We are currently living in a very dynamic society in which the economy is growing very fast due to the upcoming enterprises (SME's) which serve as a backbone to the economy. Most SME's fall victim to a limited budget plan which suppresses departments such as the IT department and depend on google services such as The Cloud where they store their data. At times, they pressure the workers to come with their devices (BYOD), which increases vulnerability by things such as viruses to the institution. Through this since most SME's need to work on a limited budget, they make time to recover from such an attack. And by this attack they could be victims of identity theft and software piracy. According to Billy Owino software, piracy undermines economic development and costs companies more in legal penalties and reputation damage. According to Staff Writer, a report by Kenyan authorities and Microsoft show that software piracy costs tech companies an estimate 128 million dollars a year and the rates are said to be as a high as 80%. Small medium enterprises attacks are on the rise also because they are ease to penetrate and cyber criminals obtain information concerning supplier networks, employee's personal information, bank records etc. for their malicious use. (Writer ,2013.)

1.3 OBJECTIVES

- To assess the number of cybersecurity measures, strategies and policies adopted by SME's.
- To determine if SME's have a team dedicated to handle cybersecurity aspects.
- Relate cybersecurity and performance of the enterprise.
- Highlights cybersecurity issues faced by SME's.

1.4 RESEARCH QUESTIONS

- How many cybersecurity measures have been adopted SME’s?
- Do they have a team dedicated to handle cybersecurity aspects?
- Has cybersecurity improved performance of the enterprise?
- What are the cybersecurity issues they are facing?

1.5 SCOPE OF THE STUDY

This research focuses small medium enterprises and how they deal with cybersecurity issues in their day to day Operations and any strategies put in place and how it affects productivity, daily operations and collaborations especially now during the covid-19 pandemic.

1.6 JUSTIFICATION

The purpose of this study is to research the small medium enterprises that are practicing cybersecurity their measures, policies implemented, highlight some of the issues they face and bring out has it has impacted their performance.

CHAPTER 2: LITERATURE REVIEW

2.1 Cybersecurity

Cybersecurity is the practice of protecting Personal computers, servers, cell phones, electronic frameworks, systems, and information from malicious attacks or is the body of technologies, processes and practices designed to protect network devices, programs and data from attack. Its otherwise called data innovation security or electronic data security. (De Groot, 2020.) Cybersecurity assumes a significant job in the progressing advancement of data innovation, just as Internet providers. Enhancing cybersecurity and securing basic data frameworks are basic to every country's security and financial prosperity, making the Internet safer. In the case of an attack, a data breach, it could very devastating effects on the organization. It could cause the organization its reputation in the market even partners. Loss of such information like licenses, source files, protected innovation. Going further, an information break can affect corporate incomes due to rebelliousness with information security guidelines. By and large, an information break cost an influenced association $3.6 million. With prominent information breaks standing out as truly newsworthy, it's basic that associations embrace and actualize a solid cybersecurity approach. (Cyber Edu, 2019.)

2.2 Types of cybersecurity

2.2.1 Application security

This is the process, which is used to toward making applications safer by discovering, fixing and improving the security of applications. Applications are much more accessible over networks, causing the adoption of security measures during the development phase to be an imperative phase of the project. (Rosenthal, 2018.) Example of this application security include an anti-virus, firewall and encrypted programs. With this type of security, unapproved access is prevented.

2.2.2 Critical infrastructure security

Firstly, critical infrastructure are systems, networks that are critical to the normal functioning of the society and economy. Some of this critical infrastructure includes hospital, traffic lights, water purification etc. Such infrastructure requires security because they are vulnerable to attacks. Organizations that are responsible for any critical infrastructure need to carry out regular checks to ensure safety and reduce vulnerability to attacks. Such infrastructure is critical to the well-being of the society.

2.2.3 Network security

This type of security is used to prevent intrusions into the organizations network of people with a pernicious expectation. Organizations have made a step ahead by using machine learning to monitor abnormal traffic and alert to threats in real time. They are also implementing policies and procedures that have to be adhered to. Examples of network security implementation new passwords, application security (encryption, firewalls).

2.2.4 Internet of things security (IOT)

According to Rosenthal, Internet of things refers to a wide variety of basic and non-basic digital actual frameworks, similar to machines, sensors, TVs, Wi-Fi router, printers, and surveillance cameras. Internet of things involve adding connectivity to a system of interrelated computing devices. By adding connectivity to devices to the internet it opens up devices to vulnerability of attacks. Hence vendors invest in studying more about challenges and suggest methods to counter them.

(Rosenthal, 2018.)

2.3 Impact of cybersecurity

2.3.1 Positive

Protect organizations networks from unauthorized access. Network firewalls are the first line of protection for traffic that passes all through an organization. (Robb, 2017.) The firewall ensures traffic that meet security requirements set by the organization.

Improved partner trust in your data security courses of action. In most businesses according to Buttler, includes 5-10% of sensitive information which if it leaked could cause loss of reputation and even revenue. (Peter Buttler, 2019.)

Quicker recuperation times in case of a breach. With cybersecurity implemented a team is set aside (IT department) to act in such times ensuring faster recovery and lesser losses incurred.

Protects Productivity-Viruses attack computers and slow down productivity and make computers crawl but by use of application security (antivirus) the risk of getting attacked are reduced to minimal.

Gives courage to employees to work safely –Generally working online you and your employees are at risk of attack from a third party, but due to the presence of a firewall vulnerability to attack is reduced.

2.3.2 Negative

Frequent software update is required for the system security to be up-to-date. The need for frequent software update is because, updated help to patch up security flaws and help you protect data. But software upgrades also change how data is handled also how it stored and cataloged. When the upgrade process is occurring the system may try to overwrite previously stored data or making a critical change. This may cause data to be corrupted or inaccessible. (Jaroop, 2019) If the firewall is not configured correctly it could limit users not to use certain sites, apps until configured correctly.

2.4 Small Medium Enterprises

According to Liberto SME's are businesses that maintain a certain level of revenues, assets and number of employees. But each country has its definition of a small medium enterprise. It has to meet a certain criteria size and the industry in which the company operates (Liberto, 2020.) He continues to explain that SME is a term commonly used by organizations such as United Nations (UN), World Trade Organization (WTO) whereas in the US they are referred to as small-to-mid-size businesses (SMB's). While in Kenya they are termed as MSME (micro, small and medium-sized enterprises). Hence this is why there is no one clear definition of what an SME is.

The SMEs are considered as the pillar of the economy, though the Information and Communication Technologies is viewed as unitary of the significant drivers for SMEs. The capacity of the ICT is to guarantee that overall, their procedure and plan, advancement of new items, administrations, measures, efficiency, extension of market size, improvement of item characteristics, upgrade of execution and, improvement, also as supporting business intensity can be executed appropriately.

In Kenya they are characterized as organizations that have somewhere in the range of one and 99 workers, which is the place where most organizations lie. According to Mputhia, the Public Finance Bill Management in 2019, proposes a meaning of SME's as an endeavor that has between 51-250 staff individuals and a turnover that doesn't surpass Sh100 million. Some challenges faced by SME's include lack of adequate managerial training. These SME owners lack adequate skills to elevate their business to the next level and achieving set objectives if there are any. Another challenge Is limited access to credit in the sense of generally in light of the fact that SMEs do not have enough collateral. Thus they think that its hard getting to capital for development. SMEs are a wellspring of numerous advancements in Kenya particularly the Jua kali area. Nonetheless, the area has not very many capital sources. Most banks won't fund developments. Bigger companies then again can go after credit as they have more insurance (Mputhia, 2020.)

In Kenya Micro and Small Enterprise authority is a state corporation under Micro and Small Enterprises Act no 55 of 2012 that was established with a mandate of promotion, development and regulation of MSE or MSME sector in Kenya (Jahkeysalma, 2020.)

2.5 Common Threats to SMEs

2.5.1 Denial of Service Attack or Distributed Denial of Service Attack (DDOS)

In this type of attack, the attack takes over many systems /devices and uses them to invoke the functions of a target system. Mainly targets websites and any form of online services. The malicious user does this by causing so much traffic to the server more than it can handle (Weisman, 2020.) The network traffic is cause by some of the following; over-subscription where a system is handling more traffic than it was designed to handle (Wilson, 2021), request for connection or fake packets. Most times a DDOS attack acts as a diversion to distract the organization as the cybercriminal continues to carry out malicious activities like stealing data or corrupting it.

2.5.2 Malware on Mobile Apps

Mobile malware is malicious software specifically designed target for example, cell phones and tablets, with the objective of accessing private information(Baker,2021.) Some common types of malware include: RATs (offers extensive access from infected devices and are often used for intelligence collection), Bank Trojans, Ransomware and advertising click fraud.

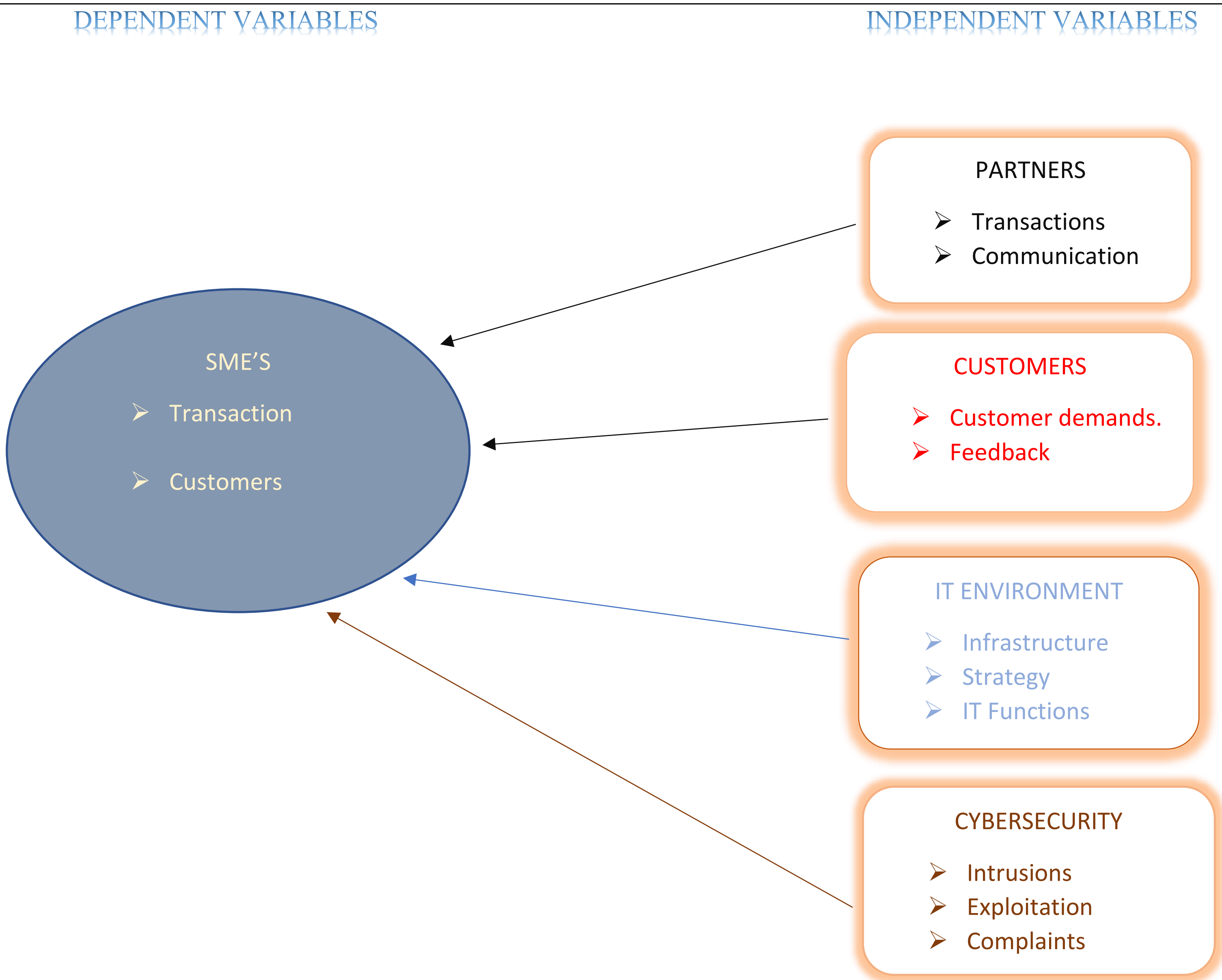
2.5.3 Phishing

This is an email-borne that tricks the recipient to reveal his/her personal information or to click a certain link to download malware. Taylor (2020.) Phishing messages are usually mass emailed to many users, where the email received looks like ‘You’ve won the lottery’ which confuse them to make the user confused and make an error. Sometimes the email comes as a blank message with a malicious attachment.

2.5.4 Ransomware

Ransomware is basically encrypting a system and demanding a certain ransom in exchange to let the user utilize the system. Taylor (2020.k,6.)

According to L. Kamau in 2017 a case called WannaCry became the worst attack so far affecting many computers locally and across the globe. Total losses from the attack were estimated to be around $4 billion. (L. Kamau, 2019.)



2.6 Conceptual Framework

In the conceptual framework, the aim is to highlight the relationship between dependent variables and the independent variables. The dependent variables consisting of; cybersecurity, IT environment, Partners and consumers all contribute to the growth and performance of Small Medium Enterprise. The independent variable is the SME under study. With that a block diagram is used to highlight the relationship.

Figure 1: Conceptual Framework

2.6.1 Partners

Factors that affect partnership between different parties include:

Transactions - This includes the capital involved to set up the business, the day to day transactions with their suppliers, consumers and the bank.

Communication - Communication is basically interaction of sending and getting messages through verbal or nonverbal methods. (Nordquist, 2019.) How does one partner communicate to the other either online or face-to-face.

2.6.2 Customer

A customer is an individual or business that purchases another organization/institution’s goods or services. (Bloomenthal,2020.) Factors affecting customers in relation to SME’s:

Customers demand-SME’s produce goods and provide services according to demands from customers to satisfy their needs and wants.

Feedback-With customer feedback it serves as a guiding resource to the growth of the company either negative or positive. (Wellington,2019.) With positive or negative feedback, you are able to determine how your customers like your goods/services.

2.6.3 Cybersecurity

As defined earlier cybersecurity or otherwise known as information security is protecting computers, servers, networks from malicious attacks. This will help highlight if the enterprise has implemented cybersecurity and if they have how is it of assistance.

Intrusions-According to Khraisat an intrusion is a kind of unauthorized access that is a threat or causes damage to a system. (Khraisat, 2019.) This implies any assault that could represent a potential danger to the data classification, honesty or accessibility will be viewed as an interruption. This could expose personal information of the company, its employees and worst case scenario that of its customers.

Exploitation-An exploitation is a piece of programming, information or grouping of orders that exploits a weakness to gain access to sensitive information. (Abi, 2020.) The aim is to get knowledge on whether the enterprise has encountered any exploitation from outsiders and how they handled it.

Complaints -Complaints are a source of dissatisfaction from one party to another. How was the enterprise able to deal with complaints from customers or workers about a particular issue?

2.6.4 Information Technology Environment

The IT environment consists of:

Infrastructure-IT infrastructure as defined by Roush is a joined arrangement of networks, hardware, software, offices, and so on (counting the entirety of the data innovation related hardware) used to create, test, convey, screen, control, or backing IT administrations. (Roush, 2020.) This IT infrastructure is meant to simplify the running of the enterprise and the researcher aim at discovering how it has been implemented.

Strategy -An IT strategy is a crucial archive that spreads out your association's capacity to make esteem utilizing IT business resources and innovative skill (Hertvik, 2020.) Any business upcoming or existent needs to have a strategy in order to meet their goals or to give upkeep, backing, and right staffing for IT situation. The IT strategy of the enterprise should be their framework to decisions and actions executed.

IT Function-This is basically where the IT department communicates with customers, suppliers etc. on issues concerning the enterprise like receiving feedback from customers.

2.7 Case Study

A research carried by Amrin Nabi out in the University of Twente Student Theses on “The Impact of Cyber Security on SME’s”. The aim of the research was to conduct an empirical study on SME’s on their security practices and position toward current technological trends. An example was Cloud computing and (BYOD)Bring your own device. The researcher uses five phases to collect data from the SME’s. First on is reviewing and synthesizing relevant literatures in order to get a preliminary conceptual idea on the most important aspects on when the SME’s IT operation was developed. Phase two a questionnaire built to ask questions. Phase three pilot interviews were conducted to test the questionnaire, one enterprise was interviewed face to face and another over the phone. The questionnaire was modified to make it simpler by describing technical terms. In phase three further SME's were interviewed. In phase four more SME's were interviewed and in phase five the researched conducted a survey to reach more SME's in different geographical locations.

2.7.1 Findings

The researcher was able to come up with questionnaires and was able to visit 16 SME's of different business operations, but registered to the government. They were interviewed on issues such as IT security trends, cybercrime victimization and cybercrime prevention practices. The researcher was able to come up with the following findings:

- For the IT security technology, the small medium enterprises implemented the use of anti-virus/malware/phishing are the most commonly used security technologies in SME's. Encrypted login sessions and keeping backups of media that show good use of IT practices.
- It security policies are not a common thing. SME's claim to have verbal rules that are undocumented rules are IT security measures and policies.
- BYOD and Cloud Computing-BYOD is accepted in SME's; the management does not have any restrictions towards employees using their electronic devices to the place of work. SME's do not controlled use of BYOD and do not anticipate any attacks on the worker's devices. In the samples collected the researcher noticed no BYOD faced any cyber threats victimization.
- Most SME's use Cloud Computing-Private Cloud is common among IT SME's and is managed by the company that uses it. None of the enterprises experienced cloud computing threats. Amrin Nabi (2014)

2.7.2 Gap identified

After reviewing the research carried out, the researcher was able to achieve his/her objectives, but the research gap comes in because no research under the topic 'A case study on the impact of cybersecurity on small medium enterprises during the covid-19 period in Nairobi county' has been carries out.

CHAPTER 3: METHODOLOGY

3.1 Introduction

Research methodology just alludes to the pragmatic "how" of any piece of research. All the more explicitly, it's about how a researcher methodically plans an examination to guarantee substantial and dependable outcomes that address the exploration of aims and objectives (Warren, 2020.) This chapter is important to this project because it provide scientifically sound findings making the research more accurate and understandable.

3.2 Research Design

Research design explains the structure of techniques and methods chosen by the researcher. There exist different types of research methods includes experimental, survey, correlational, semi-experimental and review. This study chose to implement experimental research, because it establishes the relationship between the cause and effect of a situation. Casually it observes impact of the dependent variables on the independent variable. Here primary data is used and it is obtained through interviews and questionnaires administered to the employees and managers of the organization. Since questionnaires and interview was used some of the limitations are; Interviews are time-consuming and especially now due to the covid-19 guidelines which the company is adhering to, very few people wanted to participate in the interview. For the questionnaire there is possibility of the respondents misunderstanding.

3.3 Research cite

In this part of the study, the research cite is a place where the research is conducted. In this case the SME under study is an exemplary food supplier called Bech Fresh Produce which is a local supplier of vegetables to Simbisa Brands Kenya. This part of the study is important because it introduces the SME in study to the research. The scope of this part of the study was to determine how cybersecurity is affecting their day to day activities and the strategies put in place.

3.4 Target Population

A population is an unmistakable gathering of people, regardless of whether that gathering contains a country or a gathering of individuals with a typical trademark**(Momoh,2021**.) In this case a population is a collection if elements that the researcher requires and conclusions that are ought to be made. The target population are the correspondent employees of Bech Enterprise.

3.5 Determination of study sample

3.5.1 Sampling procedure

Sampling is a process used in statistical analysis in which a predetermined number of observations are taken from a larger population(Momoh,2021.) Different methods are used by used by researchers in market research so as to reduce the workload in the sense that they don't have to research on an entire populace making it time-convenient and cost-effective. Sampling can be broadly classified into probability and non-probability. Probability sampling, the samples are selected in such a way that they are representative to the population by providing valid or credible results because they reflect characteristics of the selected population. Which include simple random sampling, systematic, stratified and clustered sampling. Non-probability sampling selection is not completely randomized hence resultant sample doesn't completely represent the population(Gaurav,2017.) which include convenience, quota, judgement and snowballing method of sampling. In order to reduce biasness, random sampling a form of probability sampling was implemented.

The research employed this method because it reduces biasness of the data which was an advantage to the study while the only disadvantage of this method was because that you may not choose enough people with your trait of interest, particularly if that characteristic is not common.

3.5.2 Sample Size

A sample is a smaller, sensible variant of a larger population. It is a subset containing the attributes of a bigger population (Kelton, 2021.) Samples are utilized in conducting a statistical study when the population is huge and it is not possible to obtain data from the whole population. According to the manager Bech Fresh produce consists of 72 workers including the management of the company. All 72 employees were issued with questionnaires concerning the cybersecurity measures of the company.

In order to obtain the sample size required, the research employed the following formulas:

$x{=}Z(^{c}/_{100})^{2}r(100\text{-}r)$

$n{=}^{N\,x}/_{((N\text{-}1)E^{2}+x)}$

E=Sqrt$[^{(N\,-\,n)x}/_{n(N\text{-}1)}]$

Where n is the sample size, E is the margin error, N is the population size, r is the fraction of responses that the research is interested in and Z(c/100) is the confidence level. The recommended sample size was 61.

3.6 Data collection measures

3.6.1 Development of instrument

This subchapter discusses instruments that will be used to collect data from the targeted SME. These are instruments are tools and devices used gather information. These include interviews, questionnaires, observation, scales and archival documents/government sources. The instrument you choose to utilize depends on the data you intend to collect either qualitative or quantitative. One of the importance of collecting data is it puts the researcher in a vantage position of being able to make predict decision about future trends and possibilities. Also it helps support the research by providing a statistical review which improves the accuracy of the research.

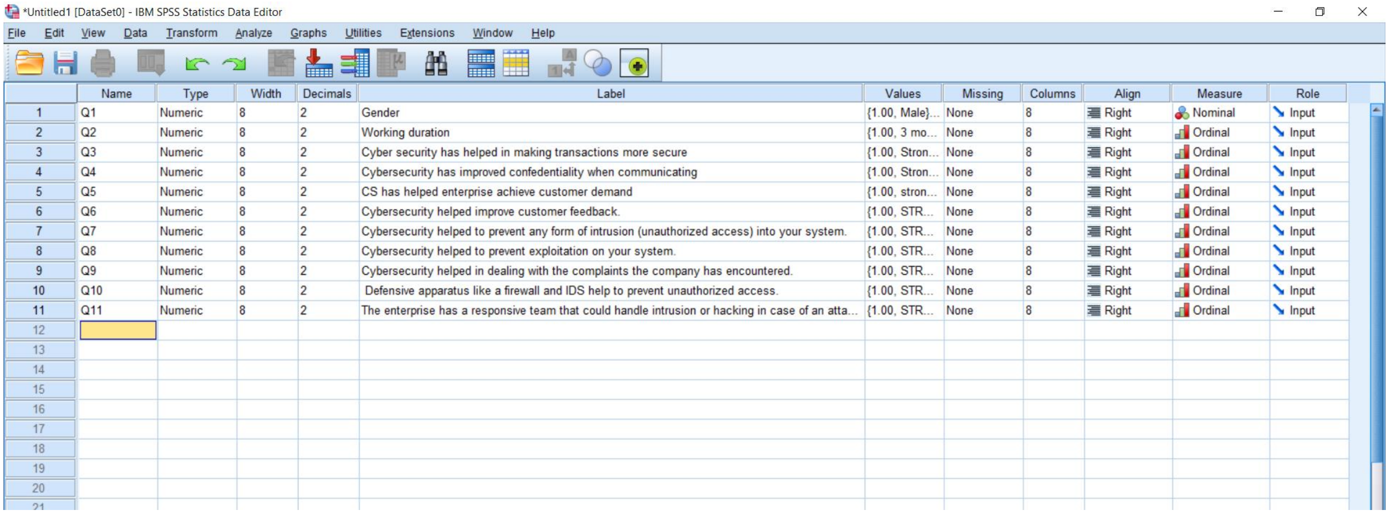
The main data collection tool in this research was the questionnaire. A questionnaire consists of a series of questions that prompts answers from individuals it is presented to. It is important to note that this is different from a survey because a survey is a process of data gathering including variety of data collection methods including a questionnaire. This research employs this method because questionnaires are easy to visualize and analyze, the respondents' identity is protected and it is relatively inexpensive. The disadvantage of this method is that different respondents have different levels of understanding and also some questions may be left unanswered due to different reasons. The questionnaire issued contained three different types of questions; the open-ended, fixed alternative and scale questions. Fixed alternative consist of yes or no questions, open-ended provide opportunity to respondent's to respond according to individual each participant's perception. Scale questions let the respondent choose on scale provided on how much they agree to the provided statement. The questionnaire was delivered personally by the researcher and the respondents were allowed to ask question on the questions not clear on the questionnaire.

3.6.2 Validity of the instrument

Validity is use to test the accuracy of the findings collected from respondents. Content legitimacy was used since it evaluates whether a test is illustrative of all parts of the develop. The questionnaire was built from the chapter 2 content especially from the conceptual framework. Legitimacy was demanded by playing out a pretest. The researcher prepared a list of questions that were meant for all employees to test their knowledge on the company's cybersecurity measures and reduce biasness on the collection of data. In the questionnaire the researcher had the choice to distinguish questions that necessary adjusting and those with ambiguities. The was then printed and dispatched to the field for data combination with the assistance of examination collaborators.

3.7 Data processing and analysis

The data collected through questionnaires was analyzed by Statistical Packages for Social Sciences(SPSS). SPSS is a powerful statistical software platform. The researcher chooses to utilize this software because it contains extensions for JAVA and it is easy to analyze and understand data in a better way.



	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	Q1	Numeric	8	2	Gender	{1.00, Male}...	None	8	Right	Nominal	Input
2	Q2	Numeric	8	2	Working duration	{1.00, 3 mo...	None	8	Right	Ordinal	Input
3	Q3	Numeric	8	2	Cyber security has helped in making transactions more secure	{1.00, Stron...	None	8	Right	Ordinal	Input
4	Q4	Numeric	8	2	Cybersecurity has improved confedentiality when communicating	{1.00, Stron...	None	8	Right	Ordinal	Input
5	Q5	Numeric	8	2	CS has helped enterprise achieve customer demand	{1.00, stron...	None	8	Right	Ordinal	Input
6	Q6	Numeric	8	2	Cybersecurity helped improve customer feedback.	{1.00, STR...	None	8	Right	Ordinal	Input
7	Q7	Numeric	8	2	Cybersecurity helped to prevent any form of intrusion (unauthorized access) into your system.	{1.00, STR...	None	8	Right	Ordinal	Input
8	Q8	Numeric	8	2	Cybersecurity helped to prevent exploitation on your system.	{1.00, STR...	None	8	Right	Ordinal	Input
9	Q9	Numeric	8	2	Cybersecurity helped in dealing with the complaints the company has encountered.	{1.00, STR...	None	8	Right	Ordinal	Input
10	Q10	Numeric	8	2	Defensive apparatus like a firewall and IDS help to prevent unauthorized access.	{1.00, STR...	None	8	Right	Ordinal	Input
11	Q11	Numeric	8	2	The enterprise has a responsive team that could handle intrusion or hacking in case of an atta...	{1.00, STR...	None	8	Right	Ordinal	Input
12											
13											
14											
15											
16											
17											
18											
19											
20											

Figure 2: Screenshot showing use of SPSS as analytic tool.

CHAPTER 4: DATA ANALYSIS, PRESENTATION AND INTERPRETATION.

4.1 INTRODUCTION

This chapter reviews the results and analysis of the qualitative data, the compilation of the questionnaires and the results and analysis of quantitative findings of the study. The discoveries are likewise examined in the light of past research findings and accessible writing, where material, in request to distinguish likenesses and contrasts between this examination and past studies and writing. An extensive depiction of the examination approach was given in Chapter 2.

4.2 Respondents demographic characteristics

4.2.1 Response Rate

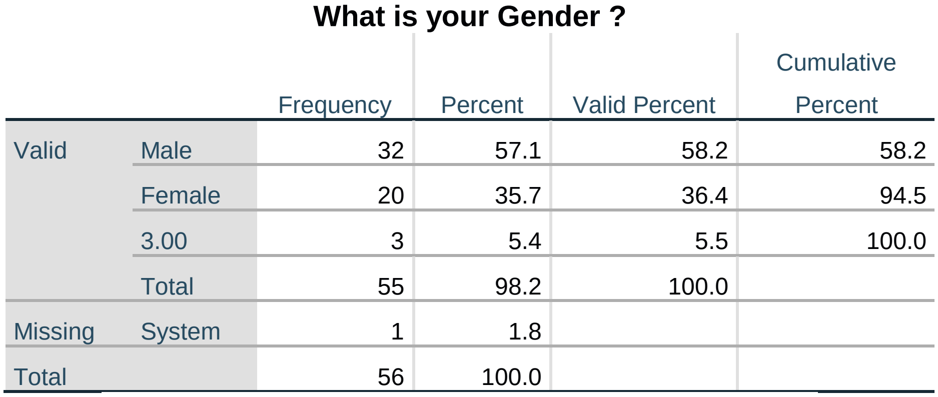
The research had a target sample size of 61 of which 55 of them responded. The response rate was 90% as illustrated in the table below.

Participants	**Frequency**	**Percentage**
Respondents	**55**	**90%**
No response	**6**	**10%**
Total	**61**	**100%**

Table 1: Response Rate

4.2.2 Gender of respondents

The study continued to investigate the gender of respondents of which 55 were male, 32 were female and the others preferred not to say.



What is your Gender ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	32	57.1	58.2	58.2
	Female	20	35.7	36.4	94.5
	3.00	3	5.4	5.5	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

Table 2: Statistics on the gender of participants.

SOURCE: SPSS

From the data collected it was observed that male was majority in the organization with 57.1% that is 32 participants whereas the females were 35.7%, 20 female participants whereas the other 3, 5.4% preferred not to reveal their gender

4.2.3 Working Duration

The workers were asked to share how long they had worked in the enterprise and were give the options of 3 months, 6 months, 1 year and more than 2 years. The responses were as following:

From the data in the table the majority of employees have worked for 3 months has a frequency of 20 (36.4%), those that had worked for 6 months were 13(23.6%), 1 year had a frequency of 10 (18.2%) and those that had worked the longest for more than 2 years were 12(21.8%).

What is your working duration in this company ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3 months	20	36.4	36.4	36.4
	6 months	13	23.6	23.6	60.0
	1 year	10	18.2	18.2	78.2
	More than 2 years	12	21.8	21.8	100.0
	Total	55	100.0	100.0	

Table 3: Responses on working duration.

SOURCE: SPSS

4.3 Presentation of Findings

4.3.1 Preference to given alternatives on the impact of Cybersecurity on SME' in Nairobi during Covid-19 Period

Both questionnaires and interviews helped to obtain data from respondents on the impact of cybersecurity based on the responses from the respondents. Employees were provided with levels of agreement on how they agree/ disagree with the provided statements. These statements are factors that affect cybersecurity.

A. Partners

The respondents agreed to their preference with the following factors on how they affected cybersecurity during the covid-19 period. Partners as a variable was plotted to obtain information on how it affects cybersecurity as a factor.

Respondents highlighted their level of agreement on the listed statements.

I Cyber security has helped in making transactions more secure.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	28	50.9	50.9	50.9
	Agree	8	14.5	14.5	65.5
	neutral	11	20.0	20.0	85.5
	disagree	7	12.7	12.7	98.2
	Strongly disagree	1	1.8	1.8	100.0
	Total	55	100.0	100.0	

Table 4: Responses of How cybersecurity has made transactions more secure

SOURCE: SPSS

In the table the first question was answered 28 participants (50.9%)strongly agreed that cybersecurity helped made the transactions between the enterprise and partners were made more secure by cybersecurity, 8 simply agreed (14.5%), 11(20%) were neutral, 7(12.7%) disagreed and 1 (1.8%) strongly disagreed.

Cyber security has helped in making transactions more secure.

What is your Gender ?			Frequency	Percent	Valid Percent	Cumulative Percent
Male	Valid	Strongly agree	19	100.0	100.0	100.0
		Agree	5	100.0	100.0	100.0
		neutral	4	100.0	100.0	100.0
		disagree	3	100.0	100.0	100.0
		Strongly disagree	1	100.0	100.0	100.0
Female	Valid	Strongly agree	8	100.0	100.0	100.0
		Agree	2	100.0	100.0	100.0
		neutral	7	100.0	100.0	100.0
		disagree	3	100.0	100.0	100.0
3.00	Valid	Strongly agree	1	100.0	100.0	100.0
		Agree	1	100.0	100.0	100.0
		disagree	1	100.0	100.0	100.0

Table 5: Frequency distribution on responses based on gender.

In the 28 participants who strongly agreed 19 were male, 8 were female and 1 preferred not to disclose their gender. The 8 who agreed 5 were male, 2 were female and 1 whose gender choose not to give out, 4 men were neutral, 7 females and 1 who did not disclose their gender. 1 man strongly disagree, 3 females and 1 of unknown gender.

Cybersecurity has improved confidentiality when communicating.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	23	41.8	41.8	41.8
	agree	16	29.1	29.1	70.9
	neutral	15	27.3	27.3	98.2
	disagree	1	1.8	1.8	100.0
	Total	55	100.0	100.0	

Table 6: Responses on impact of cybersecurity on confidentiality when communicating. SOURCE: SPSS

In table 6, 23 (41.8%) with a cumulative percentage of 41.8% strongly agreed that cybersecurity has improved confidentiality when communicating and 16 0(29.1%) agreed with the statement. The other 15 (27.3%) were neutral while 1 individual disagreed with the statement. Thus showing that cybersecurity has played a vital role in the privacy of communicating and making transactions more secure.

`

Cybersecurity has improved confidentiality when communicating.

What is your Gender ?	Frequency	Percent	Valid Percent	Cumulative Percent

Male	Valid	Strongly agree	1	100.0	100.0	100.0
		agree	1	33.3	33.3	100.0
		neutral	1	25.0	25.0	100.0
		Total	3	100.0	100.0	
Female	Valid	Strongly agree	1	33.3	33.3	33.3
		agree	2	28.6	28.6	57.1
		neutral	2	66.7	66.7	100.0
		disagree	1	14.3	14.3	100.0
		Total	3	100.0	100.0	
3.00	Valid	Strongly agree	1	100.0	100.0	100.0
		neutral	1	100.0	100.0	100.0

Table 7: Responses based on gender on impact of cybersecurity on confidentiality when communicating.

In table 7, 23 (41.8%) with a cumulative percentage of 41.8% strongly agreed that cybersecurity has improved confidentiality when communicating and 16 0(29.1%) agreed with the statement. The other 15 (27.3%) were neutral while 1 individual disagreed with the statement. Thus showing that cybersecurity has played a vital role in the privacy of communicating and making transactions more secure.

B. Customers

Customers form a huge part of the enterprise but cybersecurity helps to affirm their trust to the organization. Respondents gave their responses with the level of agreement on the statements provided. Table 4 shows the response percentage of the statements listed.

I CS has helped enterprise achieve customer demand.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	15	27.3	27.3	27.3
	agree	14	25.5	25.5	52.7
	neutral	22	40.0	40.0	92.7
	Disagree	3	5.5	5.5	98.2
	strongly disagree	1	1.8	1.8	100.0
	Total	55	100.0	100.0	

Table 8: **Responses on cybersecurity helping to achieve customer demand.**

Source: SPSS

Cybersecurity helped improve customer feedback.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY agree	17	30.9	30.9	30.9
	agree	21	38.2	38.2	69.1
	neutral	15	27.3	27.3	96.4
	disagree	2	3.6	3.6	100.0
	Total	55	100.0	100.0	

Table 9: Responses on cybersecurity helping to improve customer feedback.

In the second statement "Cybersecurity helped improve customer feedback", 15 (27.3%) strongly agreed with the statement 14(25.5%) agreed with the statement whereas 22(40%) were neutral and the other 3 disagreed and 1 strongly disagreed. So it is true to say that cybersecurity improved customer feedback to the enterprise during the covid-19 period.

C. Cybersecurity

Respondents indicated their level of agreement with the statements provided on how cybersecurity has impacted the enterprise.

I Cybersecurity helped to prevent any form of intrusion (unauthorized access) into your system.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY agree	25	45.5	45.5	45.5
	agree	25	45.5	45.5	90.9
	neutral	5	9.1	9.1	100.0
	Total	55	100.0	100.0	

Table 10: Responses on cybersecurity helping to prevent intrusion.

SOURCE: SPSS

In the first statement on whether cybersecurity has prevented any form of intrusion into the system 25% strongly agreed while another 25% were in agreement with the statement both 45.5%. 5 other respondents were neutral with statement highlighting the majority agreeing with the statement highlights that cybersecurity is vital to protect the system.

II Cybersecurity helped to prevent exploitation on your system.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY agree	28	50.9	50.9	50.9
	agree	19	34.5	34.5	85.5
	neutral	8	14.5	14.5	100.0
	Total	55	100.0	100.0	

Table 11: Responses on cybersecurity helping to prevent exploitation of the system.

SOURCE: SPSS

28 respondents (50.9%) strongly agreed with the statement “Cybersecurity helped prevent exploitation of their system”. 19 agreed while 8% one person who was neutral proving that cybersecurity has impacted them positively when it comes to exploitation.

III Cybersecurity helped in dealing with the complaints the company has encountered.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY agree	7	12.7	12.7	12.7
	agree	17	30.9	30.9	43.6
	neutral	16	29.1	29.1	72.7
	disagree	10	18.2	18.2	90.9
	strongly disagree	5	9.1	9.1	100.0
	Total	55	100.0	100.0	

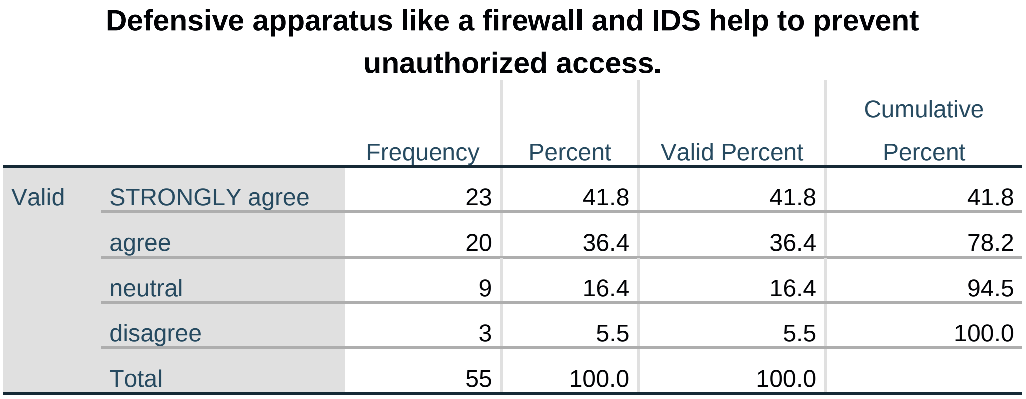
Table 12: Responses on cybersecurity helping to deal with complaints the company has encountered.

SOURCE: SPSS

Finally, in the last statement on whether the company has helped with dealing with complaints 7(12.7%) strongly agreed, 17(30.9%) agreed while the other 10(18.2%) disagreed and 5 other respondents strongly disagreed. Majority of the respondents agreeing shows that cybersecurity has impacted the positively while the 38% disagreeing have been impacted negatively. The figure below summarizes the findings.

D. IT ENVIRONMENT

The IT environment is basically the hardware and software used by the employees but in this case to practice cybersecurity. The respondents answered the following questions in accordance to their level of agreement



Defensive apparatus like a firewall and IDS help to prevent unauthorized access.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY agree	23	41.8	41.8	41.8
	agree	20	36.4	36.4	78.2
	neutral	9	16.4	16.4	94.5
	disagree	3	5.5	5.5	100.0
	Total	55	100.0	100.0	

Table 13: Responses on the presence of defensive apparatus.

In table 13, most responses were in agreement 23 having strongly agreed (41.8%) and 20(36.4%) agreeing with the statement while 9 others were neutral and 3 disagreed. With the statistics provided in the table most employees are aware of defensive apparatus in the enterprise which helps to prevent unauthorized access. The figure below helps to summarize the responses provided by the participants.

The enterprise has a responsive team that could handle intrusion or hacking in case of an attack.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY agree	29	52.7	52.7	52.7
	agree	22	40.0	40.0	92.7
	neutral	4	7.3	7.3	100.0
	Total	55	100.0	100.0	

Table 14: Responses on the enterprise having a responsive team to handle intrusion.

Majority of the responses are in agreement with the enterprise having a responsive team to handle intrusion in case of an attack with the frequency being 52.7% strongly agree, 40% agree and 7.3% are neutral.

4.4 Hypothesis

The general purpose of carrying out this research was to determine whether enterprises such as the one under study Bech Fresh Produce utilizes cybersecurity and if so if it has impacted them positively or negatively. And in conclusion from the employees who participated in the study were able to highlight that it has employed Cybersecurity which has positively impacted their enterprise and has proved very useful.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter brings forward the conclusions that undertook under this study from the previous chapters. The general objective of this research was to find out if SME's have adopted cybersecurity and the policies and measures put in place to enforce it. As for the SME in this research under case study Bech Fresh Produce Enterprise, cybersecurity was implemented especially during the Covid pandemic. Basically this chapter brings forth the findings and new information that was gathered from the research.

5.2 Summary of findings

This sub-chapter highlights the findings of the study which were driven by the objectives and research questions. The first research question being, how many cybersecurity measures have been adopted by the SME. The SME under discussion is the Bech Fresh Produce. From the questionnaires handed out to the employees, the respondents were able to give a valuable feedback which was analyzed and included in the research. The study found out that the employees were well trained with security principles, there was an employee limit to data and information, the Wi-Fi networks were secure and a firewall security for internet connection. All this were implemented whether working from home or at the business center. With the measures in place they were able to create a culture of security which enhanced business and consumer confidence.

The second objective was to determine if the SME has a team dedicated to handle cybersecurity aspects. From the questionnaires a majority disagreed that there is presence of a responsive team that could be responsible in case of an attack. This proves that the enterprise could be at a high risk of an attack especially now that majority of employees have been forced to work from home in order to comply with covid-19 guidelines. According to one of the employees, he claims that since now almost everyone is working from home, cyber attackers will take advantage of this time to attack. 47% of the working from home fall for phishing scams. The managers promised to look into the matter.

The third objective was to relate cybersecurity to the performance of the enterprise. The research question being has cybersecurity improved performance of the enterprise? This was answered by one of the managers that despite the pandemic occurring causing lockdown, the enterprise was and still is performing better with the implementation of cybersecurity. He continued to state that previously there was 63% profit and even despite the pandemic the sales have reduced but the performance now is better than before. He claims that earlier on in their working days cyberattacks were numerous and hence productivity was slowed down and at the end of the day not all consumers received their supplies. Therefore, cybersecurity has improved performance of the enterprise by boosting working conditions and security of the enterprise and therefore the have been positively impacted by cybersecurity.

Finally, the last objective and research question highlight cybersecurity issues faced by the SME and which ones are they. Firstly, the respondents claimed that it is very time-consuming to constantly update the system frequently. One of the employees stated "Sometimes you could come in the morning and the system has to update for almost two hours so that you can begin working and also it consumes a lot of memory with the constant updates. This is very inconvenient because we are suppliers who need to work with time". This was one of the respondents claiming how the updates inconvenience. Also constantly configuring the firewall can be tiring.

5.3 Conclusion

In this study, the research concluded that in order for an SME to work efficiently especially now during the pandemic it is important to note that cybersecurity is very important. Not only during the pandemic but throughout the business lifespan to protect the organization from any data losses, hacks or anything that could alter the businesses productivity. Implementing cybersecurity with workers who are not familiar with it could also cost the business. It is also important to educate the employees on standard cybersecurity procedures and measures on how to handle different scenarios.

5.4 Limitations and Recommendations

This sub-chapter discusses challenges faced while undertaking this study. Firstly, due to the Covid guidelines majority of the people worked from home. This was a challenge because reaching out to them was tough since everyone has their own schedule and people come to the work place maybe once or twice a week to avoid overcrowding. Also not all respondents managed to respond to the questionnaire.

A recommendation would be SMEs need to continue implementing cybersecurity throughout their business years. It has impacted Bech Fresh produce positively throughout the pandemic and not so many intrusions took place. It has proved its importance to the enterprise and it has boosted working performance and improved security giving customers and workers confidence to work better. Further also research needs to be carried out on the impact of cybersecurity on SME’s during the covid-19 pandemic in Nairobi county.

REFERENCE

Al Busaidi, N. S., Bhuiyan, A. B., & Zulkifli, N. (2019). The Critical Review on the Adoption of ICTs in the Small and Medium Enterprises (SMEs) in the Developing Countries. *International Journal of Small and Medium Enterprises*, *2*(2), 33-40.

Andrew Bloomentahl (2020) https://www.investopedia.com/terms/c/customer.asp “Customer”

https://www.helpscout.com/blog/customer-feedback/#:~:text=Customer%20feedback%20is%20the%20information,and%20especially)%20when%20it's%20negative.

Amrin Nabi (2014) https://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf

Cathy Mputhia Sunday (July 26th 2020)

https://www.businessdailyafrica.com/bd/lifestyle/personal-finance/why-kenya-needs-a-standalone-smes-law-2296854#:~:text=However%2C%20SMEs%20are%20defined%20according,is%20where%20most%20businesses%20lie.&text=The%20lack%20of%20a%20clear,it%20comes%20to%20SME%20legislation.” Why Kenya needs a standalone SMEs law”

Cyber Edu (2019) https://www.forcepoint.com/cyber-edu/cybersecurity "What is Cybersecurity defined, explained and explored”

Coco Dong and Michelle Hassan(2020) https://bfaglobal.com/covid-19/insights/sme-shutdown-impact-survival/ , “Short-term fixes are not enough if SMEs are to survive COVID-19”

Daniel Liberto November 14th 2020 https://www.investopedia.com/terms/s/smallandmidsizeenterprises.asp “Small and Mid-size Enterprise (SME)”

Drew Robb April 18, (2017) https://www.esecurityplanet.com/networks/network-firewalls/ “Network Firewalls: How to Protect Your Network from Unauthorized Access”.

Elizabeth Wellington (November 25,2019) https://www.helpscout.com/blog/customer-feedback/#:~:text=Customer%20feedback%20is%20the%20information,and%20especially)%20when%20it's%20negative. “Customer Feedback: Why It’s Important + 7 Ways to Collect It"

Gaurav JHA July 25, (2017) https://humansofdata.atlan.com/2017/07/6-sampling-techniques-choose-representative-subset/

“Humans of Data”

Jahkeysalma November 24, 2020.https://careerassociated.com/2020/11/24/micro-and-small-enterprises-authority-msea-internship-opportunities/ “Micro and Small Enterprises Authority (MSEA) – Internship Opportunities."

Jaroop (September 13,2019) https://www.jaroop.com/biggest-risks-legacy-software-upgrade/ “The 4 Biggest Risks of a Legacy Software Upgrade”

Joe Hertvik May 29,(2020) https://www.bmc.com/blogs/it-strategy/.” The Business of IT blog”

Juliana De Groot Monday October 5, (2020)https://digitalguardian.com/blog/what-cyber-security

Kerryn Warren, June (2020) https://gradcoach.com/what-is-research-methodology/. " What (Exactly) Is Research Methodology"

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22.

Kurt Baker - January 25, 2021 https://www.crowdstrike.com/cybersecurity-101/malware/mobile-malware/ “WHAT IS MOBILE MALWARE?”

Marc Wilson (January 19,2021) https://www.pcwdld.com/network-congestion “Network Congestion – 5 Causes & How to Alleviate Issues with your Network being Congested!"

OSIKHOTSALI MOMOH Updated Mar 18, (2021)

https://www.investopedia.com/terms/p/population.asp “Population”

Peter Buttler, June 23 2019.https://www.globalsign.com/en/blog/5-ways-to-enhance-data-security

Richard Nordquist (Sept, 2019) https://www.thoughtco.com/what-is-communication-1689877 “The art of communicating and how to use it effectively”.

Roush May 13, (2020) https://www.bmc.com/blogs/what-is-it-infrastructure-and-what-are-its-components/ .” IT Infrastructure & Components: An Introduction”

Steve Weisman (July 23.2020) https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html “What is a distributed denial of service attack (DDOS) and what can you do about them?"

Susan Ward June, (2020) https://www.thebalancesmb.com/sme-small-to-medium-enterprise-definition-2947962. “What are SME’s”

Tyas Tunngal Nov25, (2020) https://www.upguard.com/blog/exploitAbi “What is an Exploit”.

Will Kelton Jan 4th (2021) https://www.investopedia.com/terms/s/sample.asp “Sample”

Retrieved from :https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

“5 types of cyber security” Author: ND (2018)

Retrieved from: https://sites.google.com/site/xinyicyber/the-disadvantages-and-advantages-of-cyber-security Author ND

APPENDICES

APPENDIX I

LETTER TO THE RESPONDENTS

MELCHIZEDEK GICHURE

AD103890

RIARA UNIVERSITY

Dear respondents,

RE: ACADEMIC RESEARCH

I am a student at Riara University undertaking a Diploma in Business Information Technology carrying out a research on The Impact of Cybersecurity on SME's in Nairobi county during the Covid-19 period.

The questionnaire attached is however for the purpose of collecting data in this study. I humbly request you to fill this questionnaire to the best of your knowledge and ability. All the information you provide will be confidential and will only be used for academic study. Your participation is highly appreciated.

Yours truly,

…………………

Melchizedek Gichure Mwangi

Researcher

QUESTIONNAIRE

Questionnaire code: *Date: 17th March 2021*

Survey: Impact of Cybersecurity on SME's in Nairobi during the Covid-19 period.

Introduction

This questionnaire is a part of a research study being conducted on the impact of Cybersecurity in Nairobi County during the Covid-19 period. Your participation as an individual will be highly appreciated and confidential. This research is conducted for academic purposes and not a statistical study. This questionnaire is designed to identify how cybersecurity has impacted the functioning of this enterprise if it has helped to improve or deteriorate this enterprises performance.

Thankyou

SECTION A

INSTRUCTION: Please circle the appropriate answer.

Q1. Does the enterprise you represent have any cybersecurity measures/policies put in place?

A. YES B. NO

Q2. What is your gender?

A. Male B. Female C. Prefer not to say

Q3. For how long have you worked at this company?

A. 3 months

B. 6 months

C. 1 year

D. More than 2 years

Section B

Kindly indicate your level of agreement or disagreement and tick in the space allocated regarding the statements listed below.

A. PARTNERS

	1. (Strongly Agree)	2.(Agree)	3.(Neutral)	4.(Disagree)	5.(Strongly Disagree)
Did Cybersecurity help in making transactions more secure ?					
Did cybersecurity help improve confidentiality when communicating with partners and customers either on email or phone ?					

B. CUSTOMERS

	1. (Strongly Agree)	2.(Agree)	3.(Neutral)	4.(Disagree)	5.(Strongly Disagree)
Did Cybersecurity help the enterprise achieve customer demand ?					
Did cybersecurity improved customer feedback ?					

C. CYBERSECURITY

	1(Strongly Agree)	2.(Agree)	3.(Neutral)	4.(Disagree)	5.(Strongly Disagree)
Cybersecurity helped to prevent any form of intrusion (unauthorized access) into your system.					
Cybersecurity helped to prevent exploitation on your system.					
Cybersecurity helped in dealing with the complaints the company has encountered.					

D. IT INFRASTRUCTURE

	1(Strongly Agree)	2.(Agree)	3.(Neutral)	4.(Disagree)	5.(Strongly Disagree)
Did defensive apparatus like a firewall and IDS help to prevent unauthorized access?					
Did the enterprise have a responsive team in case of an attack?					