A MODEL FOR MITIGATING CYBER SECURITY THREATS AND VULNERABILITIES IN SMALL AND MEDIUM ENTERPRISES

ROSE WAITHERA KIRAGU

A Dissertation submitted in partial fulfillment of the requirements for the award of the degree of Master of Science in Applied Information Technology In the Department of Computer and Information Technology and the School of Science and Technology of Africa Nazarene University

July 2024

DECLARATION

I declare that this document and the research that it describes are my original work and that they have not been presented in any other university for academic work.

Name: Rose Waithera Kiragu

Reg No: 19J03DMIT012

Student signature: Rose Waithera Date:27th /06/2024

This research was conducted under our supervision and is submitted with our approval as university supervisors.

Supervisor name: CPA Dr. Leonard Wakoli

University supervisor signature Date:25th /06/2024

Supervisor name: Dr. Emily Roche

University supervisor signature Date:

Africa Nazarene University

Nairobi, Kenya

DEDICATION

This Research Project is dedicated to my family for their inspiration, encouragement and supports throughout my studies, May God bless you.

ACKNOWLEDGEMENT

I would like to thank the Almighty God for this opportunity and seeing me through this research thus far. Secondly, I extend my gratitude to my supervisors Dr. Leonard Wakoli and Dr. Emily Roche for their unwavering support, insights and mentorship during this research. I also thank all those that I have worked with in the course of this research. Finally, I appreciate my family and classmates for their support and encouragement

Table of Contents

List of Tables

List of Figures

ABSTRACT

Security breaches of touchy facts have remained as risk urge for food fluctuate from one company to another, it activates the chance evaluation gear be included with company`s facts protection coverage for you to make certain protection controls at The primary reason of this examine changed into to expand a version for use to mitigate cyber-protection threats in small and medium establishments. Threats and vulnerabilities confronted with the aid of using Small and Medium Enterprises, to evaluate the gear utilized in mitigating threats and vulnerabilities confronted with the aid of using Small and Medium Enterprises, to expand aversion for use to mitigate cyber-protection threats in small and medium establishments and to validate the version. Implemented each quantitative andqualitative study. Data was gotten using purposive sampling from Small Medium Enterprises and was analyzed using SPSS model 26 and Python. Discoveries have been that the modern-day contraptions for risk appraisal paperwork have now no longer blanketed statistics protection association for possible protection management primarily based totally on company`s hazard. The want of compelling risk evaluation primary sources which includes servers and purchaser wise devices at the hand of assailants and on this manner increment risks and chance to compromise the sources. The examine determined that vulnerabilities, authentication mechanism and schooling stood out because the unbiased variables from the coefficient examine achieved with the aid of using python making the researcher drop infrastructure competencies and facts protection coverage. Made have been that Small Medium Enterprises preserve to put in force cyber security to Small Medium Enterprises and has progressed paintings overall performance as nicely as to paintings better. Further studies are wanted on a comprehensive version to mitigate cyber security threats in Small Medium Enterprises in Kenya, strategies,demanding situations and great practices in Nairobi. Version to mitigate cyber security threats in Small Medium Enterprises in Kenya.

DEFINITION OF OPERATIONAL TERMS

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Small Medium Enterprises: unified, programmed application software which helps organizations to maintain multiple transactions at one place.

ABBREVIATIONS AND ACRONYMS

CIA:	Confidentiality, Integrity, Availability
COBIT:	Control Objectives for Information and related Information Technology
ERP:	Enterprise Resource Planning
InfoSec:	Information Security
ISACA:	Information Systems Audit and Control Association
ISMS:	Information Security Management System
ISO:	International Organization for Standardization
IT:	Information Technology
MFA:	Multi-Factor Authentication
NIST:	National Institute of Standards and Technology
SFA:	Single-Factor Authentication
SSO:	Single Sign-On
TFA:	Two Factor Authentication

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Cyber security is the security of data and computerized resources from compromise, burglary or misfortune. The assault can be from a decided assailant exterior, or an insider risk inside your trade. It is security because it relates to the dangers of being online (The Australian Small Business and Family Enterprise Ombudsman, 2017). According to Castro (2018) small businesses confront critical cyber security danger. In 2015, the National Small Business Association reported that 42 percent of small businesses were casualties of cyber intrusions. It also found that on average, cyber-attacks cost small businesses about $7,000, and when their bank accounts were hacked, their average loss was about $32,000. Small businesses generally face the same types of threats as large businesses, but small businesses are more likely to encounter certain types of cyber incidents, such as malware and phishing attacks.

Furthermore, in 2017, 58 percent of confirmed data breaches involved small businesses (Castro, 2018). Small and medium- sized enterprises represent "soft" targets because they are less protected, unaware of the risks, and often not even aware of them can detect the extent of theft in the cyber environment. Due to the increase in these types of threats, the development of effective preventive security systems is more necessary than ever. At the enterprise level, it's not just a simple or arbitrary attack that causes damage. On the contrary, many attacks have lasting consequences. Today, targeted attacks to misuse sensitive data, remove copyrighted material or simply steal it have become more common. This type of attack can disrupt a company's operations for days or months, d a m a g e i t s reputation, or even jeopardize its operations. His existence as the use of IT tools increases in Small Medium Enterprises, companies have more opportunities to attack from several different directions. (Small Medium Enterprises, 2021).

1.2 Background of the study

The COVID-19 pandemic has accelerated digitization worldwide and forced companies such as Small Medium Enterprises to make rapid and drastic changes. These include implementing cloud services, updating internet services, redesigning websites and enabling employees to work remotely.

This paradigm shift has created an environment where cybercriminals and threat actors pose a significant threat to homeland security. Cyber security failure is considered the fourth most likely risk to become a major global threat in the near future.

A common misconception is that cyber-attacks only happen against large organizations because they contain elements of greater interest to criminals, such as large financial data belonging to customers or sensitive and valuable intellectual property. Contrary to popular belief, all organizations, regardless of size, can be attacked in the same way, especially Small Medium Enterprises, because they have different risk/reward ratios and higher profits.

Many Small Medium Enterprises also provide services to larger organizations and can therefore provide criminals with the opportunity and resources to attack these larger organizations, disrupting the supply chain. Criminals are also particularly targeting small and medium-sized businesses, knowing that many businesses struggle to maintain adequate cyber security as they rapidly move to remote work and implement the IT systems needed to run your business. Small and medium-sized businesses are increasingly dependent on digital technology. However, unlike large companies, they cannot acquire and implement complex cyber security solutions and expertise.

This exposes them to serious digital security risks and increases the likelihood of becoming a victim of a cyber-attack. Many employees of small and medium- sized businesses have little or no knowledge of cyber security.

It is often assumed that cyber security threats concern only IT professionals, leading to a common understanding of the risks and impacts of a cyber-attack. In fact, many phishing attacks, such as email phishing, take advantage of this ignorance and thus prove to be an excellent tool for initial compromise.

1.3 Statement of the Problem

Cyber security threats are on the rise, posing significant risks to small and medium enterprises (Small Medium Enterprises) in Kenya. Data breaches, phishing

attacks, ransom ware, and malware are becoming more frequent and sophisticated, challenging the ability of Small Medium Enterprises to protect their data and operations. A trend analysis shows a steady increase in reported cyber-attacks against Small Medium Enterprises in Kenya. 54% in 2020, 58% in 2021, and 64% in 2022. This upward trend is a significant concern, as Small Medium Enterprises often lack the resources and expertise to effectively manage cyber security threats.

Small and medium enterprises (Small Medium Enterprises) in Kenya do play a very crucial role on the country's economic growth as well as development. However, these businesses are increasingly vulnerable to cyber security threats due to limited resources, inadequate security infrastructure, and a lack of cyber security awareness. Unlike larger corporations, Small Medium Enterprises often lack dedicated IT teams and the financial resources to implement robust cyber security measures. This vulnerability exposes them to various risks, including data breaches, malware attacks, ransom ware, and other forms of cybercrime this is according to the data from European Economic and Social Committee, 2018 (European Economic and Social Committee, 2018).

According to Castro (2018), most small businesses are concerned about cyber security but they do not do enough to protect themselves against cyber security threats. The majorities 58% of small businesses are concerned about cyber threats, a third "do not take any proactive measures to protect against cyber threats" and half "do not allocate any budget to risk mitigation services". One reason for this lack of action is that many small businesses underestimate the potential risk they face from a cyber-attack due to lack of awareness.

IBM noted in its 2014 Cyber security Intelligence report that in more than 95% of incidents, human error was a contributing factor, from poor password protection to misuse of passwords. Internet connection is not secure. A recent publication by Hoffmann Bedrijfsrecherche B.V a Dutch fraud investigation office, noted that due to such negligence, security checks were able to penetrate three out of four companies. Five prominent security vulnerabilities include predictable passwords, unused server connected to the Internet, website weaknesses, "legacy data" that is available but forgotten, such as backup code and source code. Lack of use of security protocols can be addressed through training and user awareness (frinking, 2023)

As compared to corporate institutions, small business enterprises do not have the budget to afford, purchase or install the highest security measures. Given such

absence of security guards, sophisticated monitoring systems, and technically equipped entry devices give way to cybercriminals to attack without fear. An example is when hackers plant malicious software on business computers to be able to capture online banking credentials such as logins and passwords which they can later use to gain access to the given company applications (Xiaoyun Wang, Advances in Cryptology, 2012).

The problem is exacerbated by the rapid adoption of digital technologies and e-commerce platforms, driven by the need for operational efficiency and growth. Despite this digital transformation, many Small Medium Enterprises are not adequately equipped to deal with cyber risks, lacking comprehensive security strategies, dedicated IT personnel, and cyber security training. This vulnerability not only jeopardizes the survival of Small Medium Enterprises but also threatens the broader economy, given the substantial role Small Medium Enterprises play in employment and GDP contribution in Kenya (Xiaoyun Wang, Advances in Cryptology, 2012).

This study endeavored in creating a model for mitigating cyber security threats and vulnerabilities in small and medium enterprises. Once these factors are established, the developer of the security solution will incorporate these factors into the technical solutions hence making the technical solutions holistic.

1.4 Purpose of the study

The goal of this study is to develop a comprehensive model for mitigating cyber security threats and vulnerabilities in small and medium enterprises. This model aimed in providing Small Medium Enterprises with practical, cost-effective strategies to enhance their cyber security posture, reduce vulnerabilities, and protect their data and operations. The model addressed the unique challenges faced by Small Medium Enterprises in Kenya, focusing on prevention, detection, response, and recovery from cyber threats.

1.5 Specific Objective

i. To assess the current state of cyber security in Small Medium Enterprises in Kenya, including common cyber threats vulnerabilities.
ii. To analyze existing solutions to the cyber security threats and vulnerabilities facing Small Medium Enterprises in Kenya.
iii. To develop a cyber-security mitigation model tailored to the needs and constraints of Small Medium Enterprises in Kenya.

iv. To validate the research model through pilot implementation and feedback from participating Small Medium Enterprises.

1.6 Research Questions

i. What are the threats and vulnerabilities faced by Small and Medium Enterprises?
ii. What are the existing solutions to the cyber threats and vulnerabilities faced by Small and Medium Enterprises?
iii. What are the ways of designing and developing a model which will be used to prevent cyber security threats in small and medium enterprises?
iv. What is the best way of validating the model developed?

1.7 Significance of the Study

The main recipients of this study's benefits are Kenya's Small Medium Enterprises. Small Medium Enterprises who will be better able to defend themselves against cyber-attacks, guaranteeing business continuity and lowering the possibility of monetary loss and reputational harm by offering a thorough cyber security model.

i. Associations for the Industry and Business Groups: These entities might utilize the results to create initiatives that assist Small Medium Enterprises in enhancing their cyber security procedures. The results of this study helped in advocating for cyber security laws that help small and medium-sized businesses.
ii. Politicians and those who set policy. The study's conclusions can help government organizations develop laws and policies that promote cyber security in small and medium-sized businesses. Additionally, it can help national cyber security plans that cater to Small Medium Enterprise's needs.
iii. Academic Community will use this study can be utilized by scholars and researchers.

1.8 Limitations of the Study

This research will be carried out against the following limitations.

Small Medium Enterprises are several in Kenya and are typically located in each and every corner of the country, hence creating a challenge in physical access during data gathering. This will be moderated sufficiently by the effective use of anelectronic survey to tentatively reach the Small Medium Enterprises.

During the academic study, the COVID-19 pandemic led to the imminent closure of Small Medium Enterprises, new ways of typically carrying out tasks online and social distancing. This will be moderated by the use of an electronic survey to ensure the data is collected while observing the new measures.

Small Medium Enterprises vary in size, infrastructure, population among other factors, which influence the systems they use and systems security challenges. This will be moderated by conducting the survey based on their current systems and infrastructure and the popular breaches which are faced by them.

1.9 Assumptions of the Study

This research will be conducted under the following assumptions:

i. The interviewee will provide truthful, accurate and reliable facts to the best of their knowledge.
ii. Information Technology experts are best placed to provide information on authentication of the given Small Medium Enterprises systems used in the different companies and therefore the survey will only cover the common security breaches which are faced by the given companies.
iii. Literacy levels of users in these institutions are adequate for the implementation of the anticipated secure the Small Medium Enterprises systems.
iv. The respondents will be able to provide data for the study while adhering to privacy policies and the sensitive nature of information systems security. The survey to be conducted will allow for anonymous responses and in line with the organizational privacy policies.

1.10 Cyber Security Models

1.10.1 NIST Cyber Security Model

Concurring to (Vasileiou, 2019) The National Institute of Standards and Technology (NIST) Cyber security Model (NIST CSF) is a United States (US) policy model that provides information security guidance to help organizations assess and improve their ability to resist cyber-attacks. It is not a prescriptive standard, but aims to define a common language and a systematic approach to cyber risk management.

To achieve this, it is divided into a model core with five key functions that define the key stages of asset and threat management namely; detect, protect,

identify, respond and recover. These activities were then divided into 22 categories (Vasileiou, 2019).

These classes are then divided into subclasses with approximately 100 security features that are actually related to other standards such as ISO 27001, COBIT, NIST SP 800-53, and ISA 62443. Therefore, the use of the NIST CSF is really a reference model that combines different approaches and also allows a transition from one approach to another. It aims to create a broad and stable foundation for cyber security.

The NIST Cyber security model needs. It does not provide the government with an acceptable level of cyber risk that a company may or may not tolerate, or a mythical "all-in-one" model to prevent cyber-attacks. However, it explicitly allows best practices to become standard methods for all through a common vocabulary that allows activities to be shared among different stakeholders (Vasileiou, 2019).

The NIST CSF also provides an incremental level of implementation. It provides context for how the organization views cyber security risks and processes for managing those risks. This model can be practically applied by small and medium-sized companies.

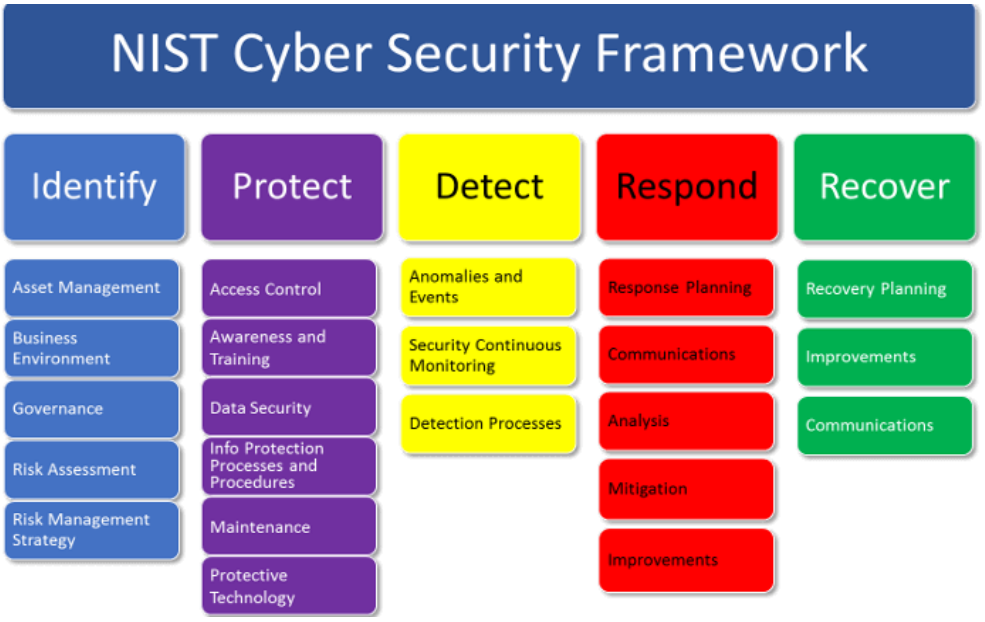


Figure 1: NIST Cyber Security Model (Vasileiou, 2019)

The NIST CSF also has provided a progressive implementation tiers. It has provided the context on how an organization views cyber security risks and shared the ways in place to manage those risks. The model can realistically be used by Small Medium Enterprises (Vasileiou, 2019).

Figure 1.2: NIST Cyber Security Model Tiers (Vasileiou, 2019)

1.10.2The Stands for Systems and Organization Controls 2 (SOC2)

SOC 2 can be a security model that showed how organizations should protect customer data from unauthorized access, security breaches and othervulnerabilities. The model was developed by the American Institute of Certified Public Accountants (AICPA) focusing on five areas; security, availability, processing integrity, confidentiality and privacy (NDNB, 2024). The SOC 2 report is tailored to the unique needs of each organization. Each organization can design guidelines that follow one or more trust principles according to its business processes. These internal reports provide organizations and their regulators, business partners and suppliers with important information about how the organization manages its data (Imperva, 2024). There are two types of SOC 2 reports:

Type I report presents the organization's systems and whether the system design meets the relevant trust principles.

Type II report described the effectiveness of certain systems.

SOC 2 security principles focus on preventing unauthorized use of assets and data handled by the organization. This principle requires organizations to implement access control measures to prevent malicious attacks, unauthorized data deletion, misuse, unauthorized modification or disclosure of company data (Imperva, 2024).

The following is a basic SOC 2 compliance checklist that includes security standards checks:

Access Controls - These are the logical and physical settings of an asset to prevent unauthorized access.

Change management - a controlled process to manage changes and methods to IT systems to prevent unauthorized changes.

System Functions - Commands that can be used to monitor daily operations, identify and resolve possible deviations from organizational methods.

Risk Mitigation - Methods and activities that enable an organization to identify, respond to and mitigate risks when dealing with potential subsequent transactions.

It should be noted that the SOC 2 criteria do not describe exactly what an organization must do - they can be modified according to the needs of the business. Companies must take responsibility for the selection and implementation of control measures according to certain principles (Imperva, 2024).

SOC 2 compliance is a headache for many organizations, but achieving ongoing compliance and reducing annual frustration is within your reach. In practice, there are four processes that lead to ongoing SOC 2 compliance:

Step 1: Define your scope.

The first step to SOC 2 compliance is to define the scope. The AICPA has established five key fiduciary service criteria that a SOC 2 audit should consider. These criteria are based on the existing systems and processes in the organization: not all SOC 2 assessments must consider all five categories. Next, determine which systems, policies, and procedures support the appropriate principles. Other aspects of scope include the systems involved (e.g., application or service, people, location or entity, technology) and the overall project timeline from start to finish (Imperva, 2024). (Valli, 2014).

Step 2: Gap Analysis and Control Mapping.

Conduct a monitoring readiness assessment to identify gaps between your trust services criteria and your internal monitoring environment. This determines whether your current controls are sufficient to meet the auditor's SOC 2 expectations. Conducting a gap analysis or readiness assessment prior to an audit can help you reduce remaining gaps, enabling a more efficient audit process (Imperva, 2024).

Once you've put your controls together, map your control environment to the

trust services criteria and start collecting relevant documents, such as policies and procedures. Conscious control mapping is a sign of a well-planned and comprehensive control structure. The mapping also meets the needs of platform management so that they can document the controls in use to meet SOC 2 criteria.

Step 3: External reporting.

Finding a good SOC 2 audit partner is essential. Only a CPA firm can perform your SOC 2 audit, but that doesn't mean every CPA firm is perfect for an audit. Find a CPA who understands the specific needs of your industry and organization. By establishing a relationship with third-party auditors who conduct their own independent tests and report whether they agree with management's claims, your organization will achieve SOC 2 certification (Imperva, 2024).

Step 4: Technology to support ongoing compliance.

Many organizations treat SOC compliance as an annual exercise, but the landscape of cloud-based monitoring can change rapidly. Applying a GRC arrangement to manage compliance allows you to control the model, identify and monitor control gaps, collect evidence for certification and report to management. If SOC 2 audits are reviewed throughout the year, there should be no surprises during the next certification period and review. Subsequent compliance with SOC 2 should be key, as controls were continuously monitored. The focus shifts to the gradual accumulation of recorded evidence (Imperva, 2024).

1.10.3 Audit Objectives for Information and Related Technology (COBIT)

COBIT was developed by the International Association for Auditing and Control (ISACA), an international professional organization for people interestedin IT auditing. IT Risk and IT Management. ISACA was founded in 1967 and has grown into a global organization managing 150,000 employees worldwide. COBIT was originally created to support accounting (financial) professionals in an increasingly dynamic environment (De Haes, Van Grembergen, & Debreceny,2013).

ISACA published the first version of COBIT in 1996 as a template for conducting IT audits. The first version was quickly followed in 1998 by a second version intended for the comprehensive management of IT processes.In 1998, ISACA recognized the growing importance of IT in business and the

growing need for effective IT governance, and established the IT Governance Institute (ITGI), a management consulting organization.

The knowledge gained from ITGI contributed significantly to the development of COBIT as an ideal IT management and governance model (Valli, 2014). Based on the revision of the first two versions, COBIT developed a more comprehensive IT management model.

The third version of the COBIT model was released in 2000 and included management principles (including metrics, critical success factors, and an IT process maturity model). In 2005, ISACA launched COBIT 4.0, which introduced several new concepts for leadership and management, such as aligning businessand IT goals and their relationship with IT support for processes, and roles and responsibilities in IT context were working. Computer processes and relationships between computer processes Conceptual Model. This fourth edition aims to establish COBIT as an accepted IT management model.

The conceptual model shows the independent and dependent variables for the study. A comprehensive model for mitigating cyber security threats to small and medium enterprises in Kenya strategies, challenges and best practices the independent variable, perceived measures, is based on vulnerabilities, authentication methods, infrastructure, compatibility, information security policies and user training. The dependent variable, Small Medium Enterprises cyber security compliance threats model, is based on the CIA triad that addresses information system security with respect to confidentiality, integrity, availability, inaddition to system related factors on usability and attack tolerance.

The conceptual model constructs were derived from the National Institute of Standards and Technology (NIST) Cyber security core framework, the theories. Theory of planned behavior and the Augmented Protection Motivation theory as follow:

i. NIST infrastructure capabilities and Authentication mechanisms.
ii. Augmented protection motivation theory
iii. Vulnerabilities and training.
iv. Theory of planned behavior
v. Information security policy

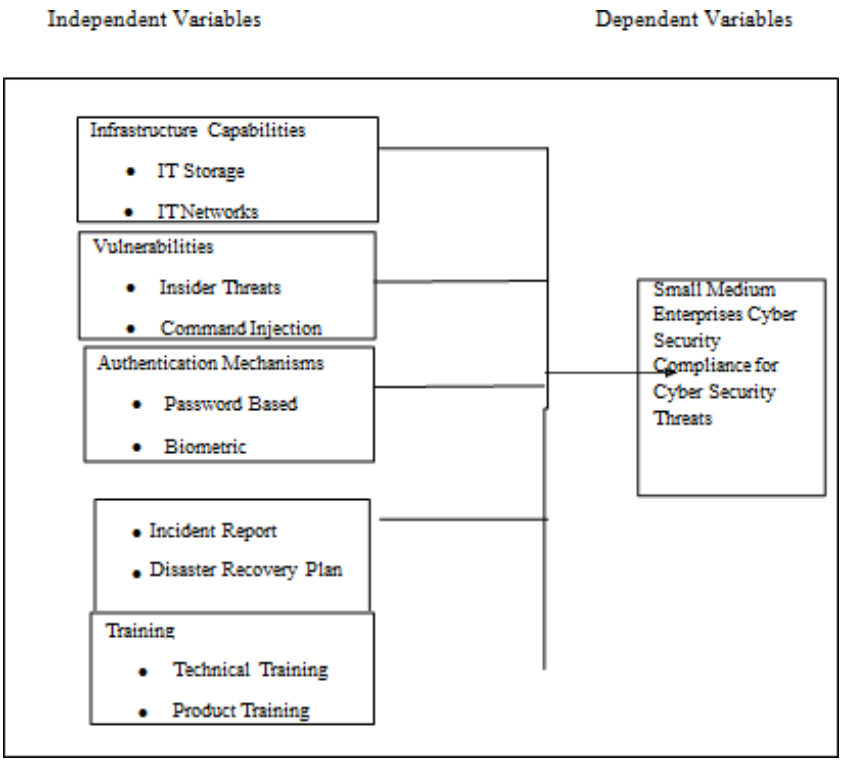


Figure 1.3: Conceptual Model (Researcher, 2024)

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews related literature categorized into sections derived from the research objectives. The purpose of this research is to develop a comprehensive model for mitigating cyber security threats to small and medium enterprises in Kenya strategies, challenges and best practices

2.2 Review of the Literature

Small businesses are different departments, going from a one- person small business to a 50-50-person company to access the internet uniquely. If you use the Internet and save something important on your computer or phone, you are at risk. She sheds light on how small business owners are struggling and how they can make small changes to their online presence.

Small businesses are less likely to have an online control system, so they admit they are more secure online or admit they don't need internet security. Small businesses often don't have a dedicated IT team or management, so cyber security isn't a practical task. This false sense of security increases the risk of small businesses being exploited by attackers and the "insider threat" that arises from a lack of knowledge or consideration of insider transactions (Mccluskey, 2017).

The resources of small and large businesses are exposed to the risk of cyber-attacks, such as data breaches, information deletion and denial of access to information, which can impact operations. However, there are many signs thatsmall and medium-sized businesses are reducing cyber risks by not using security measures. While most experts agreed that cybercrime is the biggest problem facing all businesses, small and medium- sized businesses believe they are not immune to its choices.

Furthermore, cybercrime estimates are considered very challenging due to the large number of unreported and undetected cyber incidents. Small and medium sized businesses have become prime targets for cyber-attacks. This is due to weak protection strategies, less skilled skills and outdated security technologies

compared to large companies. Although some small businesses are aware of the risk of cyber-attacks, they may suffer from these incidents because of the need for energy, the need for resources, and the need to be careful (Alahmari A, 2020).

Furthermore, estimating cybercrime is particularly difficult because many cybercrimes go unreported and undetected. Recently, an understatement in official reports is that small and medium sized businesses have become prime targets for cyber-attacks. In most cases, the main reason is the ineffectiveness of the preventive measures used by small and medium-sized companies compared to largecompanies, as well as a lack of skills, a lack of external clarity and outdated security strategies.

Many small businesses underestimate the fact that they can recognize the potential of cyber-attacks, but the need for energy, resources and power leaves them vulnerable in such cases (Alahmari A, 2020).

2.3 Theoretical Model

2.3.1 Technology Acceptance Model (TAM)

The Technology Perception Model (Kasper Hornbæk, 2017) emerged from theories of intentional action and planned behavior. The use of the technology consent model has expanded to include many technologies beyond computers, including (Rebecca Schnall, 2016), digital technologies (Rebecca Schnall, 2016), mobile application (K, 2020), and online learning platforms for students (K, 2020).

The technical consent model has been extended to include additional predictors to add efficiency and ease of use. An extension is to incorporate perceived risk (Pavlou, 2016). Technology risk perception is defined as the extent to which a person perceives the use of technology as threatening (Rebecca Schnall, 2016). In the technology acceptance model, as risk increases, the intention to use a technology decreases.

An example is the creation of training programs for new technologies. Once you identify the new skills you want to promote, your TAM can guide you in designing a training program. For example, if you know that ease of use is a key driver of adoption, you can create training materials that emphasize the usability of your app and provide step-by-step instructions for using the app.

Also, knowing that usability is important, you can demonstrate the benefits of your app and present case studies or farmer experiences. Other people have used this program successfully to improve their results.

2.3.2 Diffusion of Innovation Theory

The diffusion of innovation (DOI) theory presented by Rogers (1983) may be a commonly utilized hypothesis that shapes the establishment for considers on selection and dissemination of IT advancement (Lyytinen, 2003). It has been recognized that the recognition of advancement by decisions-makers influences their slant to receive a modern item (Rogers, 2009). It is advance proposed that relative advantage; compatibility, complexity; trial ability and discernibleness are five development characteristics that have an effect on the recognition of advancements both emphatically and contrarily (Rogers, 2009).

The writing demonstrates that the hypothesis of DOI is well set up and the five characteristics have been conveyed effectively in a few considers almost IT development selection (Lyytinen, 2003). Seen relative advantage such as ease of utilize and financial motivating forces has uncovered to have a positive effect on appropriation choices (Lyytinen, 2003)

Compatibility and complexity had noteworthy affect to the selection of fabric prerequisite arranging measures (Zmud, 2022). Premkumar et al. (1994) found that specialized compatibility and relative advantage essentially expanded the rate of appropriation of electronic information compatibility arrangements. In the interim, Bradford and Florin (2003) did not discover any critical impact of technical compatibility in their thinking about the usage of endeavor assets arranging frameworks which demonstrates that there are a few shortcomings to the consistency of what DOI thinks about as well as the accuracy of it (Kasper Hornbæk, 2017).

To address such shortcomings, a few analysts have combined it with other hypotheses, permitting for a more agent-based system that addresses the interaction between state of mind, deliberateness and behavior. Post-adoption hypotheses, such as innovation acknowledgement, and hypothesis of arranged behavior have been executed to address people pre- and post-adoption discernments (Kasper Hornbæk, 2017).

In cyber security, the DOI hypothesis has also been actualized. In considering the person's appropriation of anti-spyware program, the analysts found relative advantage, compatibility, perceive ability and trial ability to be critical components in shaping an individual's state of mind towards anti-spyware program (Younghwa Lee, 2008). In any case, ease of use was not noteworthy at all. In a ponder, almost the individual's selection of computer data frameworks security measures, the discoveries recommended that convenience and ease of use were not found to have a huge effect on purposeful to utilize the measures (Younghwa Lee, 2008).

The authors speculate that due to security measures regularly being obligatory, the impact of ease of use and value isn't as solid, which is negating writing but in line with what comes about from the thought about the selection of anti-spyware software. Besides, within the setting of security, organizations may emphasize more on securing themselves against vulnerabilities instead of advancing ease of use and convenience as key drivers. The second objective was well represented by this theory since it showcased the most prevalent cyber security threats facing Small Medium Enterprises and their impact on business operations.

Other variables, such as administration bolster and preparing back, did appear to have a positive impact on the deliberate to embrace (Jones et al., 2010). Whereas effectively utilized in IT advancement, Hameed et al. (2012) have tended to another impediment to DOI other than irregularity. It is often used to consider the behavior and state of mind of individuals within the selection of advancement and fails to clarify the total advancement selection. Hence, the DOI hypothesis alone may well be lacking to fully clarify the appropriation of advancements in organizations (Marie-Laurence Caron-Fasan, 2020).

2.3.4 General Deterrence Theory

The hypothesis proposes how people can be discouraged from doing unscrupulous self-centered activities with consequences, such as strict obstacles and punishments in connection to them. It is conceivable to require countermeasures like preparing and mindfulness programs, reinforcements, and fiasco recuperation measures to dispense with the dangers and diminish thosedangers. Discouragement exercises bolster activities that counter the criminal infringement of the internet through awareness raising measures for clients of the internet (Schuessler, 2009).

The center components of the common discouragement hypothesis are discouragement, anticipation, and location and cure (Schuessler, 2009). The chance administration approach to cyber security straightened out by the Common Deterrence Theory makes it the proper column for this ponder because it pointed to create a system that guarantees way better administration of the internet and clients assurance against cyber-attacks which aligns with our third objective. The diagrammatical presentation of the theory is as shown in Figure 2.3

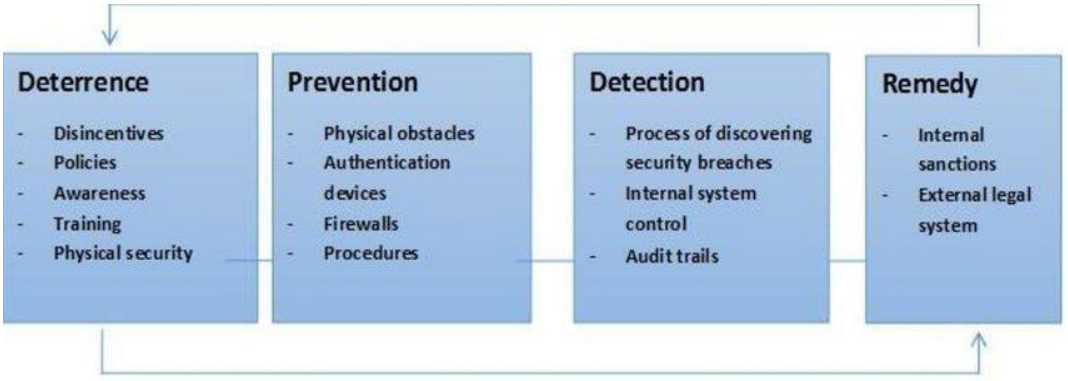


Figure 1.4: Elements of the General Deterrence Theory Alanezi et al (2014)

2.3 Implemented Cyber Security Program

A cyber security program can be a series of exercises, security measures and security audits designed to prevent and quickly and fully recover from a productive cyber-attack on an organization. The program must ensure confidentiality, integrity and availability (CIA) validation of systems and information involving the IT resources of the organization (Norman, 2023).

Cyber Security Program Benefits depend on each organization's unique business, development environment and threats. Several trusted industry codes and councils, such as NIST, ISO and OWASP, support the information and make it available to those who depend on program organization and management.

With rules and robust planning, a certain level of responsibilities can be defined for all experts in the organization, and IT security monitoring is implemented, monitored and controlled by the IT group or a separate security meeting. Cybercrime is becoming dynamically overwhelming, targeted and costly.

According to an IBM report, businesses incurred nearly $6 trillion in cybercrime victims in 2021, with data breaches typically costing $5.4 million per incident in 2021. Cyber-attacks are associated with downtime, damage to brand reputation, resulting in fewer connections and potentially large volumes. Fines or accepted claims.

In one case, third-party software vendor Kaseya experienced a ransomware attack that used a supply chain attack to deliver ransomware to the customer's victim systems.

Trusted Revil Group presented a translation request of 70 million dollars. Influential information. The Kaseya ransomware ambush underscores the importance of monitoring security breaches to identify them and develop quick and effective response plans to mitigate their negative effects.

Thus, instead of the routine ROI calculation, the condition ROSI (Return on Safety Speculation) should be used, which confirms the speculative number of safety events avoided.

ROSI = (Security Sought, preserved in Vital Removal - Shrinkage Achieved) / Avoidance Sought Rationally calculating the benefits of essential isolation in addition to the costs, the theory of a cyber-security program can be more clearly legitimized and the organization. Can benefit from the program to survive the cyber breach storm.

2.3.1 10 Steps to Creating a Winning Cyber security Program.

Creating and managing a Cyber security program allows for operational flexibility. However, organizations must calculate and apply relative risks and concentrations in an organized manner, rather than relying on an ad hoc open. For Small Medium Enterprises, a reasonable cyber security program must be implemented to ensure sensitivity. By creating an exchange, it can evolve its program to meet the needs of changing security situations (Norman, 2023).

A 10-step approach provides a solid path to building a cyber-security program from the ground up:

i. Assessing Cyber security Capabilities
ii. Choosing a Cyber security Framework
iii. Creating a Cyber security Model
iv. Building Cyber security. Company Information Security Policy
v. Security Approaches and Management Measures
vi. Protect Your Orchestration
vii. Protect Your Data
viii. Protect Your Applications
ix. Test Your Information Security Posture

x. Research and Explore the Scope of the Development Program.

From now on, organizations must continue to improve and advance their cyber security program to achieve true ongoing cyber resilience.

Step 1: Conduct a security risk assessment

The risk is not reliably present throughout the organization. Every business has important forms and assets that support its operations. The purpose of a security risk study is to isolate critical forms and assets and assess their suitability to implement security measures and controls to ensure the quality of operations.

An organization's significant area of risk may also depend on important national titles such as GDPR for companies that store Personally Identifiable Information (PII), HIPPA for companies that store Personal Health Information (PHI), and industry standards such as PCI. -DSS for companies that specifically process prepaid card data. (Stevens, 2024).

The threat assessment includes adverse control measures and industry fines or other control measure

Step 2: Choosing a Cyber Security Framework

After a random assessment, the organization can choose the most appropriate cyber framework system to mitigate cyber risk based on the results of the risk assessment.

A cyber security system is a guide to making the best choice. In planning and implementing arrangements and supervision. In many different cases, using an IEC 18 key controller can be a very expensive and impractical system for small businesses.

Other common cyber security standards include:

i. ISO-27001 / ISO-27002
ii. NIST Cyber Security Framework (CSF)
iii. Center for Critical Cyber Security Controls (CIS-CSC)

In some cases, companies must adhere to a specific standard, such as PCI-DSS for Enterprises, which specifically regulates remittance cards, or Cyber security Mature Model Certification (CMMC) for logged-in users. With the US Department of Defense (DOD).

Domestic controls may also require companies to take proactive measures to protect customer data, such as GDPR for EU-based organizations and HIPAA for US organizations handling personal health information (PHI).

Step 3: Create a cyber-security approach

A cyber security program can be a never-ending and iterative process. A cyber security procedure can be a formal contract or manual that establishes a standard for a company's information security program and plans exercises for the next 2-3 long periods. (Norman, 2023). Including creating a cyber-security method.

Formation of teams

i. Allocation of parts and tasks
ii. Allocation of assets
iii. Conducting target turns
iv. Conducting focused exercises

Focused exercises that included

i. Improvement of organization and security controls
ii. Testing
iii. Verification
iv. Research methods
v. Weak filtering
vi. Penetration tests
vii. Security-conscious preparation

By further organizing the program, the organization can ensure the reliability of information security ongoing, contains risks and dangers over time.

Without a well-organized and ongoing process, efforts are more likely to revert to ad hoc protection (dataguard, 2023)

Step 4: Develop a security risk management plan

Each organization's situation is unique and will evolve with the time. Organizational of security skills is an iterative tool that often re-evaluates the relative risks of an organization.

It licenses the prioritization of resources and forms so that resources are properly allocated and risks managed through appropriate cyber security policies and regulations that meet the unique conditions of each company to Cyber security

- Advisory Forms (Fujitsu, 2023).

SMB may need to implement a comprehensive IT Risk Management Framework (RMF) to ensure best practices are followed in managing the opportunity.

Some common IT risk management frameworks are:

i. NIST SP 800-53 RMF
ii. SO 31000 RMF
iii. COBIT 5
iv. CERT-RMM

Step 5: Establish security policies and controls

Organization and controls help to characterize standard operating procedures (SOP) that inevitably ensure the best aspects of IT security for the selected cyber security system and remain vigilant.

The most important way to define the core work of IT security approaches and management methods is to ensure:

Confidentiality - access to information by unauthorized persons or frames is not possible.

Integrity - Data cannot be changed by unauthorized persons or cadres.

Availability - when needed, internet frames can be continuously restored during rest (because they reside outside of a storage medium such as hard drives, removable drives or cloud resources), data in transit (because they have beenexchanged) and data. In use (because they are produced in the CPU and RAM).

Securing these core components must include regulatory, specialized, and physical approaches and controls designed to isolate, prevent, and recover from episodes that otherwise appear to compromise an organization's IT framework and business operations as deploy a successful-cyber security plan (Norman, 2023).

Step 6: Protect Your Network

Contract security included protecting data during the contract by deploying and designing next-generation firewalls in addition to security. Each contract endpoint (Fujitsu, 2023).

Critical areas of the organization's topography have deployed next-generation firewalls to securely operate deployments and endpoints. Next-generation firewalls unlock the capabilities of traditional firewalls and are qualified to use advanced orchestrated security features such as:

i. Outage detection and waiting.
ii. Object filtering, which allows you to take a closer look at records and isolate them with detected malware.
iii. URL filtering restricts websites within an organization.
iv. Performing standard firewall functions such as port restriction by

installation.

Applying Continuous Vulnerability Management Techniques to manage the removal of vulnerabilities exploited by an attacker, organizations continuously assess their weaknesses within the organization.

Another important component of organizing weaknesses is the happy foundation of software patches, which ensure that updates are combined with fixes for vulnerabilities in operating systems and computer programs discovered bymerchants themselves (Norman, 2023).

Advanced vulnerability management programs use penetration tests to ensure that strong security features are reasonably protected and cannot be bypassed by an attacker. Additionally, it is important to note that industry standards such as PCI-DSS and SOC-2 may require ongoing audit, vulnerability and penetration testing.

Install Endpoint Security products

Because the foundation of the organization combines both the data carriers that enable the movement of information between systems and the systems themselves, exceptional organizational security requires the security of both.

Some endpoint security issues, such as common malware scanners and other demo-day and advanced endpoint detection and response (EDR) practices, are available and must be addressed on endpoints to reduce disease (Advisory, How to Implement an Information Security Program in 9 Steps, 2024).

Figure 2.4: Endpoint security items (Valli, 2014)

The biggest advantage of EDR functionality is that it can proactively screen for system indicators of compromise (IOC), rather than simply scanning entries for malware when it arrives at the endpoint.

Designing information security elements is too imperative for pre-designated IT people to monitor, investigate and implement progress where necessary (Guidance, 2021).

Step 7: Protect Your Data

Data can be a critical asset in an exchange operation, and failure to properly protect data can leave an organization vulnerable to ransom ware attacks and/or cause internal fact theft. Of the main business. Once the information is identified and classified according to its level of impact, decision makers can choose which forms of verification to combine (Guidance, 2021)). Let's look at some security aspects.

Implementing Data Incident Prevention Strategies Data Incident Expectation (DLP) combines several key approaches to prevent data theft from escaping an organization. A handful of techniques used to prevent data problems include Scrambling data at rest.

Using remote wipe capabilities on flexible devices (tablets, phones and tablets). Activation of removable media restrictions (preventing or controlling the use of removable USB drives and optical media.

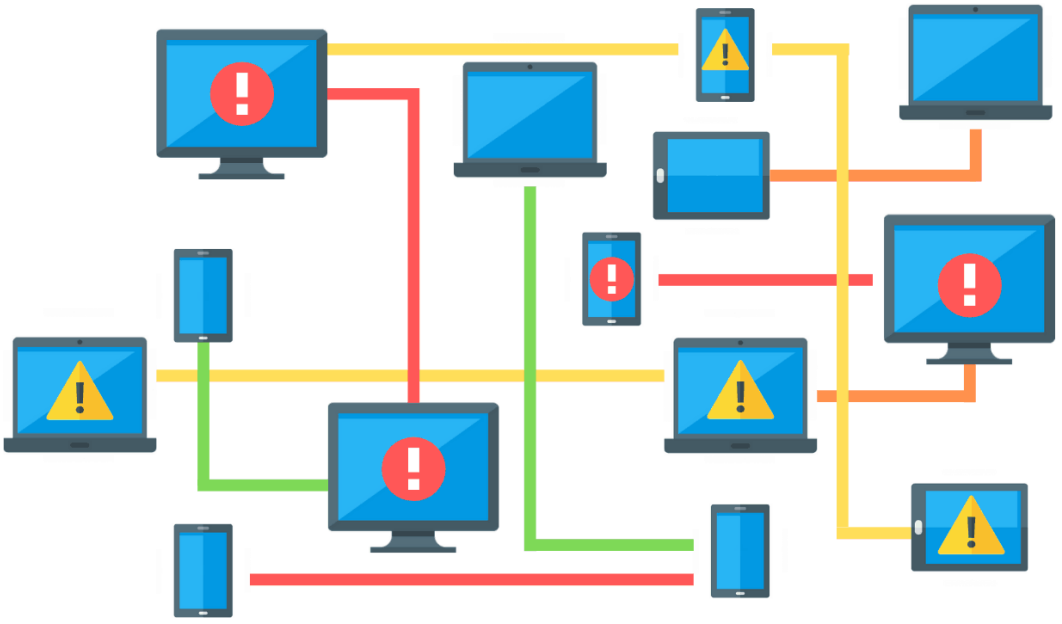


Figure 2.5: Data Loss Prevention Strategies (Guidance, 2021)

When it comes to DLP within an organization, next-generation firewalls can be

designed to funnel and degrade weak drives so they don't filter out of the organization. A DLP approach can further combine the latter approaches, such as a "least privileged" approach that ensures that access to data is granted to the individuals and systems that need it, and "segregation of duty" that bypasses everyone's allocation.

The questions are worked down to the smallest detail to ensure that the debtor and liquidator do not focus on one person or small group (Guidance, 2021).

Implementation of the Strengthening Agreement

Strong and practical support measures are needed to continue to operate trade ambiguity. It must be associated with citadels that store data in many packages and at different stages of their life cycle, such as:

i. Endpoint disk images
ii. Servers
iii. Cloud-based resources such as Virtual Private Servers (VPS)
iv. Isolated shutdown of databases, applications and other records

A shutdown strategy should strive to ensure that satisfactory time objectives (RTO) and recovery points (Fujitsu, 2023). This allows an organization to change its authentication method, bypassing potential questions if necessary. Finally, strongholds must be removed from multiple regions, the smallest of which supports advanced out-of-region enhancements like Assault, which mitigates data loss due to disgruntled riders.

A data/disaster recovery plan is in place

Knowing how to organize and implement disaster recovery can be the difference between a minor outage and a long-term disruption that can have a lasting financial impact (Guidance, 2021).

Ransom ware attacks are advancing every day, but a well- thought-out recovery organization ensures that IT personnel know how to fully and quickly recover a variety of ransom ware data and supporting systems. Recovery operations help plan IT forces and provide confidence that incident recovery can be done quickly and efficiently, reducing the slippage caused by the momentum of an actual cyber breach event.

Implementation of Security Awareness Training Communication channels such as email, social media and other private advisory systems are a direct way for attackers to display malicious records or join an organization's organization

(Fujitsu, 2023). Attackers can trick experts into signing orders or clicking orders using advanced social engineering techniques called phishing or phishing attacks that use settings to gain a broad view of an organization.

True-blue design allows personnel to monitor real-world communications and drive awareness between real-world communications and phishing ambushes, and take action if they suspect they are being targeted (Fujitsu, 2023).

Step 8: Protected Applications

Software is the equipment that supports the operations of an organization.
It is also true that application exploits are the first common vector abused by external attackers to gain early access to an organization's configuration. Let's takea look at the many important ways Small Medium Enterprises need to secure their applications (Norman, 2023).

Get basic business applications. Changes in computing make business more complex and lead to higher costs and risks, so costs and risks can be reduced if Small Medium Enterprises outsource significant capacity to an IT service provider. Monitoring a mail server can be a difficult task with basic results (Norman, 2023).

If an organization's email server is compromised, the company may lose the ability to communicate with customers, have its emails encrypted with ransom ware, destroyed or stolen. Arises from the business of privileged insights during the accident. After that, many Small Medium Enterprises outsource their email management to a vendor. As office applications spread to the provider's cloud environment, records are conveniently available anywhere, easily shared and collaboratively used, and approvals are naturally under merchant control (Norman, 2023).

Use multi-step verification. Stolen passwords and brute force password cracking are some of the most important traps used. Protection against client-side attacks is multi-factor authentication (MFA). MFA provides strong control by requiring the customer to confirm a one-time passcode (OTP) delivered to the corresponding device or by examining the USB device ID. Yubikeys is our favorite tool in today's program (One login, 2024).

Limit the application base to the necessary attackers who can exploit the software being used. Application whitelisting is a way to declare a list of approved programs in each frame and ensure that no other applications are displayed (Guidance, 2021)

Whitelisting applications reduce the number of ambushes by limiting the ways an attacker can initiate a plan. Adding application whitelists can also help control what options are available to an attacker, as many attackers use LOTL privileges. If you use devices pre-installed with a working system and do not use abuse tools, you can activate a security warning (Heimdal, 2023).

Step 9: Test the Security Posture

Organizing and implementing access and control is the heart and soul of a cyber-security program. Anyway, all that hard work is for nothing if you just don't stick around and practice (Fujitsu, 2023). Shields provide all aspects of a potential ambush surface, while cyber attackers must find a single vulnerability to defeat.

Security control scope testing enhances legacy systems incompatibility testing and monitoring to ensure security policies are defined. Sophisticated testing strategies combine penetration testing with a set of highly heated exercises where cyber-attacks against the orchestra are recreated to test real-world defenses (Fujitsu, 2023).

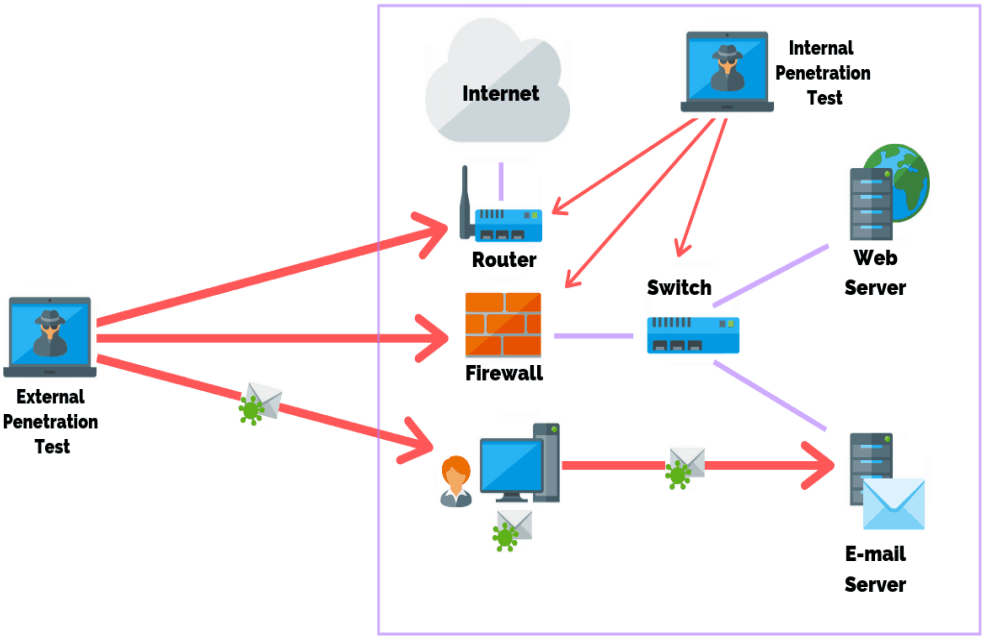


Figure 2.6: Testing the security pose (Fujitsu, 2023).

Penetration testing and red team works out too serve to test a security team's capacity to distinguish and authentically direct noxious behavior on the organize and its endpoints

Step 10: Evaluate and Improve Program Effectiveness

The cyber peril scene and trade operations are both progressing circumstances that make they require for modifications to a cyber-security program. Subsequently, a cyber-security program ought to be an iterative prepares to preserve its resiliency.

Overview the reasonability of the program since it stands: Survey the viability of the program because it stands. Recognize potential ways to streamline the program.

For outline, checking can show up that cyber ambushes are concentrated, or where the level of hazard has changed (Fujitsu, 2023). The assessment stage may be an awesome time to require note of vital triumphs and deliver advance reports that can serve to prompt top-level bosses around the cyber security programs' practicality and ranges where more resources may be required.

Figure 2.7: Four Steps to building a cyber-security strategy (Guidance, 2021).

2.3.2 Summary of Review of Literature and Research Gap

Different investigate works have been conducted on cyber security chance administration by distinctive creators where they have had diverse discoveries that can offer assistance in this ponder. Agafonov and Damkus (2017) investigated the hypothetical perspectives of the cyber security administration demonstrate that can be utilized to guarantee the security of basic framework in any organization or company.

The discoveries of the inquiry about demonstrated that the cyber security

administration demonstrates. It should always include six measurements. Those measurements are valid directions, coincidence administration, greatadministration, innovation administration, security, culture, and occurrence administration, which provide support to downplay the risks and limit the impact ofsuccessful cyber-attacks.

Additionally, it can be initiated against the organization's foundation and help us have an enhanced awareness of the security situation both inside and outside the company. The majority the concept presented in the article about the cyber security administration show is that the organization as a whole need to prioritize cyber security, and every department within the Cyber security must involve organizations.

The study conducted by Haufe, Colomo-Palacios, Dzombeta, Brandis, and Stantchev (2016) focused on data security administration for constructing, carrying out, operating, and monitoring examining, monitoring, and advancing the data security of an organization and suggested .The highest level of commitment in this study is an SMS handle system.

The framework was founded on based on an established set of SMS procedures in current measures similar to the ISO 27000 arrangement, COBIT and ITIL.Within the system, notable forms were represented, and their interfaces and communication were indicated. It was intended for the proposed system to help.

Small businesses should focus on how the SMS operates rather than on metrics and governs. Using data security hazards as a focal point, Montenegro and Moncayo (2016) explored governance in order to assess and reduce the risk of data security in Small Medium Enterprises. As they for the purpose of evaluating and reducing the chance of data security breaches in Small Medium Enterprises. The suggested demonstration included OCTAVE-S and ISO 27005 generalization mechanisms system.

In South Africa, Kabanda et al. (2018) carried out research on SME cyber security. And the difficulties they face in establishing new countries. The overall goal was to make experts and government educators more aware of the difficulties and obstacles faced by Small Medium Enterprises so that the different parties can work collaboratively in giving context-specific arrangements to address these challenges and progress current cyber security hones.

The thought about taken after a subjective request approach to request data from three South African Small Medium Enterprises that had executed cyber security

hones. The discoveries appeared that an SME's perception of cyber security is obliged by inner components of budget, administration back, and demeanors.

Encourage comes about appear that Small Medium Enterprises cyber security hones are influenced by the scene of cyber security, as well as regulation weights. Kljucnikov, Mura and Sklena (2019) conducted a study to recognize the components of victory of data security administration in portion of Small Medium Enterprises in Slovakia.

Checking that the information security organization complies with the company's exchange policies, security controls, organizational mindfulness, and back of beat organization were identified by the analysts as the four key success factors of the information security organization. The investigation's disclosures demonstrated that strong security measures.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides an overview of the research methodologies used by the researcher to conduct the study. The chapter discusses research design, population and sample, data collection methods, research methods, and data analysis methods.

3.2 Research Design

The research design plan shows the structure of the techniques and processes chosen by the researcher. Several different research methods are available, such as experimental, survey, correlational, quasi-experimental, and survey.

Using a descriptive research method, the researcher identified the research topic a comprehensive model for mitigating cyber security threats inSmall and Medium Enterprises Kenya Strategies, Challenges and Best Practices and the objectives presented in Chapter 1.3. The first part of the survey consists of a series of well-structured questionnaires in the participating organizations. Another aspect is done by creating a model that clearly shows the purpose of the study.

3.3 Target population

The significance of the study is determined by the accuracy of the data. By selecting the right population and implementing an exposure test design, accuracy is likely to be achieved (Kumar, 2011). According to Cooper and Schindler (2012), a population is a set of basic questions about which a researcher should make suggestions.

3.4 Target group

The research group consisted of ICT Small Medium Enterprises operating in Nairobi. The target group included 190 ICT Small Medium Enterprises recruited to operate in Nairobi. The list of these Small Medium Enterprises was obtained from the Kenya Business Directory (Directory, 2023).

3.5 Research sample

Sample planning is a structure that forms the starting point for choosing a research test (Lavrakas, 2008). Model design is crucial to choosing the right model.Think of the test as fulfilling a purpose, not as a one-sided test.

Sample size is a research term used to determine the number of representative individuals included in a study. Sample size refers to the total number of respondents who participated in a study, and this number is often divided by demographic information such as age, gender, and location to make the total sample representative of the entire population.

Among the 190 ICT Small Medium Enterprises, the sample size of the study was found to be 98 ICT Small Medium Enterprises, which was derived from the Cochran's formula equation, which is considered particularly suitable in situations where the population is large. Cochran's formula is:

Cochran equation

$$n_0 = \frac{Z^2 pq}{e^2}$$

Where n_0 is the sample size,

Z^2 is the abscissa of the normal curve that cuts off an area α at the tails;

(1 – α) equals the desired confidence level, e.g., 95%);

e is the desired level of precision,

p is the estimated proportion of an attribute that is present in the population,and q is 1-p.

The value for Z is found in statistical tables which contain the area under the normal curve. e.g Z = 1.96 for 95 % level of confidence

Where:

n = the smallest sample size

Z = 1.96, i.e. the level of significance determined by the 95% confidence interval corresponding to a Z-value of 1.96

p = the proportion of the target population of the total population that was estimated to have the measured characteristics.

Q = variable calculated as (1-p)

d = acceptable error rate (determined in this study) Therefore, the sample size for

this study was calculated as follows:

$n = 1.96^2 \times (0.069) \times 1 - 0.069)$

0.05^2 n=98

The sample size of the formula was ninety-eight (n=98).

3.5.2 Sampling Procedure

The researcher used purposive sampling strategy. Creswell (2014) suggests being purposeful in identifying participants that might provide insight into your research question.

Purposive sampling refers to intentionally selecting participants based on their characteristics, knowledge, experiences, or some other criteria. Participants are chosen on "purpose," not randomly. It is also known as judgmental sampling or selective sampling.

For the researcher to get meaningful feedback the IT department personnel who deal with the software, networks and databases were the targeted participants.

3.6 Data Collection Method

This study used primary and secondary data collected through a structured online survey designed by the researcher based on the objectives of the study. Questionnaires are often designed for a specific study to collect different types of information, such as people's opinions or attitudes. It is a flexible tool to use because it allows you to collect feedback from multiple participants without having to talk to everyone (Cooper and Schindler, 2012). Data were collected over a period of three months.

3.7 Pilot Testing of Research

The objective of the study was to develop a comprehensive model to mitigate network security threats, strategies, challenges and best practices for Small Medium Enterprises in Kenya. A pilot survey was conducted among IT Small Medium Enterprises in Nairobi County with 9 respondents (10% of the sample size). The area was chosen because it has similar characteristics to the study area. Pilot studies are an important step in increasing the accuracy and clarity of data collection tools. All questions appear to have high reliability as indicated by Cronbach's alpha coefficient greater than 0.7. Therefore, all questions are considered reliable from the point of view of the study

3.8 Instrumental Reliability

Instrumental Reliability The qualitative test was measured by Cronbach's alpha coefficient to determine the internal consistency of the items used in the study. All questions appear to have high reliability as indicated by Cronbach's alpha coefficient greater than 0.7. Therefore, all questions are considered reliable fromthe point of view of the study

3.9 Validity of the instrument

Validity is used to check the correctness of the results collected from the respondents. Content validity is used because it assesses whether the experiment describes all aspects of the development process. The questionnaire was prepared from the content of Chapter 2 and especially from the conceptual framework.

Legality requires prior research. The researcher created a list of questions for all employees to test their knowledge of the company's cyber security measures and minimize bias in data collection. In the questionnaire, the researcher has the opportunity to distinguish between questions that require correction and ambiguous questions. The questionnaire was then printed and sent to the field for data collection with the help of assessment partners.

3.10 Data collection process

Data collection was done through questionnaire which were both printed and sent via Google forms. The respondents were able to read by themselves and later filled back the questionnaire which later were collected by the researcher. The purpose of sending the questionnaire via Google forms was that it is low on cost and that it reaches a wide geographical population. Also respondents have adequatetime to give well thought out answers. Large samples can be made use of and thus the results can be made more dependable and reliable.

3.11 Data analysis

Data analysis is the process of cleaning, analyzing, interpreting, and visualizing data using various techniques and business intelligence tools. Data analysis tools help one discover relevant insights that lead to smarter and more effective decision-making. The research compiled data from the questionnaire such as age, gender, outdated software, multifactor authentication etc. This raw data was then

interpreted through SPSS and Python to show relationships between the different variables.

3.12 Legal and Ethical Considerations

The researcher obtained permission from the African Nazarene University to conduct this study. Permission was also obtained from the ethical board. The researcher received a license from the National Commission for Science, Technology and Innovation (NACOSTI). The researcher then obtained consent from the participants to confirm their interest in the study. In this case, respondents were asked to read the consent form and confirm whether they agreed to participate. Participants were informed that participation in the study was voluntary and that they could withdraw from the study at any time if they could no longer participate. In addition, the researcher confirmed the confidentiality of the data through an affidavit.

CHAPTER FOUR

RESEARCH AND ANALYSIS

4.1 Introduction

These chapter presents data analysis and research results. The questionnaire used in this retrospective study was carefully analyzed to ensure that the data collected were clearly presented through tables, percentages and graphs where possible. Retrospective chart analysis was performed to collect information relevant to the study objectives. The overall objective of this study is to create a model to mitigate cyber security threats to Small Medium Enterprises in Kenya. The questionnaire consisted of four sections with a total of 22 structured closed questions, which were designed to ensure that each section and the objectivity of the data are well presented of.

4.1.1 Age and Gender

From the data present the two genders which were presented (males and female). The male had the highest presentation with an age of above 46.

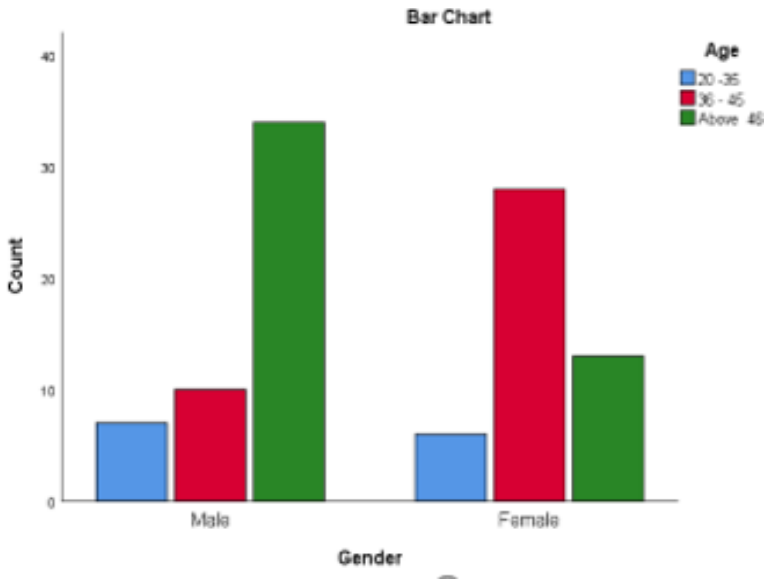


Figure 2.8 Age and Gender (Researcher, 2024)

4.1.2 Threats Faced

From table 4.1 we can be see that 50 respondents stated no with 51% and 48 respondents representing that threats play a significant role in cyber security threats. Agreed that there was a relationship amongst the threats faced.

Table 4.1 Threats faced (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	50	51.0	51.0	51.0
	Yes	48	49.0	49.0	100.0
	Total	98	100.0	100.0	

4.1.3 Outdated Software

There was a 50 – 50% percent which indicated that the companies were using software being used was outdated.

Table 4.2 Outdated Software (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	49	50.0	50.0	50.0
	No	49	50.0	50.0	100.0
	Total	98	100.0	100.0	

4.1.4 Policies to educate employees about cyber security

The respondents had 50 – 50% knowledge on about having policies to educate them about cyber security. This was viewed as a nice gesture since some had made the steps but it was not indicated when and if till date the education was shared amongst the employees.

Table 4.3 Policies (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	49	50.0	50.0	50.0
	No	49	50.0	50.0	100.0
	Total	98	100.0	100.0	

4.1.5 Strong password being enforced

There should be a need to come up with strong passwords since all the 98 respondents amounting to 100% stated there are no strong password being enforced.

Table 4.4 Strong Password (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	98	100.0	100.0	100.0

4.1.6 Small Medium Enterprises engagement with third-party vendors

There was 50 – 50% on the sensitivity of the data which was being shared by the third party vendors

Table 4.5 Engagement with third party (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	49	50.0	50.0	50.0
	No	49	50.0	50.0	100.0
	Total	98	100.0	100.0	

4.17 Antivirus used

53 respondents amounting to 54.1% stated that their companies did not use antivirus making it a major issue since they are dealing with sensitive information as well as third party vendors from the previous data gathered.

Table 4.6 Antivirus (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	45	45.9	45.9	45.9
	No	53	54.1	54.1	100.0
	Total	98	100.0	100.0	

4.1.8 Risks prioritized based on their potential impact on the organization

From the total 45 people stated that the risks are prioritized and the majority being 53 stated that no they are not prioritized, this is quit risky since this number might be the cause of Small Medium Enterprises closing done hence the importance of coming up with the model.

Table 4.7 Risks prioritized based on their potential impact on the organization (Researcher, 2024)

	Observed N	Expected N	Residual
Yes	45	49.0	-4.0
No	53	49.0	4.0
Total	98		

4.1.9 Process for evaluating, improving the effectiveness of the framework

The 98 respondents stated that there was no process of evaluating and improving the framework hence there be a need of coming up with a model to assist them

Table 4.8 Evaluation and improvements of the framework (Researcher, 2024)

	Observed N	Expected N	Residual
No	98	98.0	.0
Total	98[a]		

4.1.10 Designated incident response team.

There was no response team set aside for handling cyber security incidents and they did not as well have a process for regularly evaluating and improving the Model effectiveness.

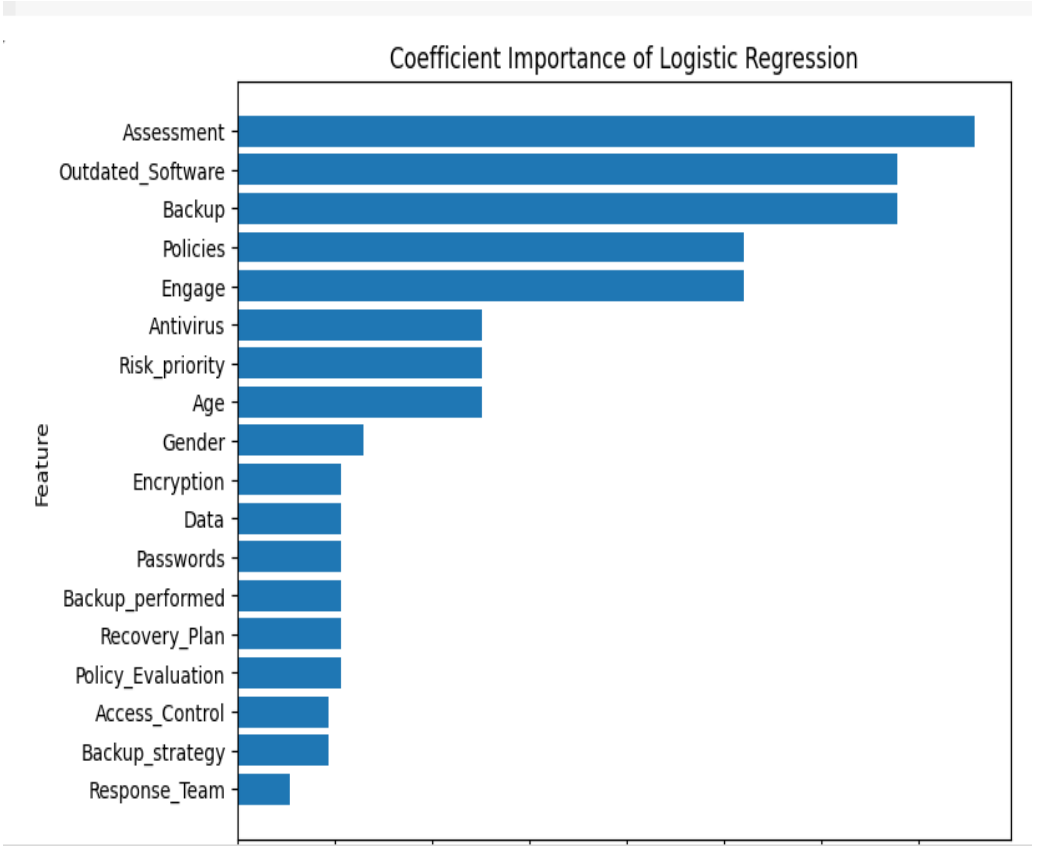
Table 4.9 Response Team (Researcher, 2024)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	98	100.0	100.0	100.0

4.1.11 Process used to drop some of the model

The researcher used python to do the analysis for showcasing the coefficient importance of the questionnaire and it showcased the strength to the least strength of the coefficient. Assessment, Outdated Software, Backup, Policies and engagement were see as the major areas which will be used in coming up with the model Recovery plan, Policy evaluation, Access Control, Backup strategy and response team was ranked as the least hence making the researcher drop the Infrastructure Capabilities and Information Security Policy as the independent variables.

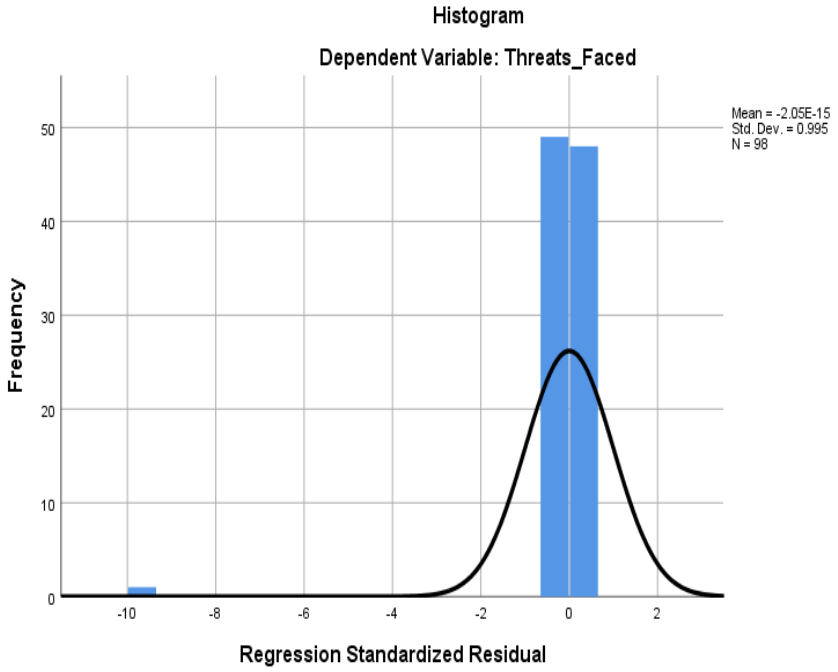
Table 4.10 Coefficient importance of logistic regression (Researcher, 2024)



4.1.12 Histogram

The researcher tested this assumption by reviewing the histogram of standardized residuals for the dependent variables infrastructure capabilities and information security policy against the dependent variable threats faced. The residuals were approximately abnormally distributed, as displayed in our histogram below; the assumption was not met hence stating the need to come up with the model.

Table 4.11 Histogram indicating how infrastructure capabilities and information security policy was dropped (Researcher, 2024)



4.1.13 Independence of observation Durbin-Watson statistic in the model summary (Researcher, 2024)

The researcher displayed the value of the Durbin-Watson statistic in the model summary table to determine whether our data satisfies the independence of observations assumption. Values between 1.5 and 2.5 are normally considered to satisfy this assumption. Our value of 1.022 falls below the range.

4.2 SMEs Cyber Security Compliance Model for Small and Medium Enterprises

The procedures followed during the development of the proposed security compliance framework for Small and Medium enterprises are described. To model the linear relationship between the independent variables and the dependent variable in the conceptual Model depicted in Figure 1.3 in Chapter one, Multiple Linear Regression analysis performed. The formula for this Multiple Linear Regression is stated as follows:

`x

$Y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \ldots \beta_n x_n + \varepsilon$ eq. (1)

Where:

$Y =$ Dependent variable

$x_i =$ Independent variables

$\beta_0 =$ The y-intercept (constant term)

$\beta_i =$ Slope coefficients for each independent variable

$\varepsilon =$ Model error term

Based on Figure 1.3, the dependent variable is **SMEs Cyber Security Compliance** while the independent variables are: Infrastructure Capabilities, Vulnerabilities, Authentication Mechanisms, Information Security Policy and Training.

Hence, eq. (1) is modified as follows:

$Y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 + \varepsilon$ e eq. (2)

Where:

$Y =$ SMEs Cyber Security Compliance

$x_1 =$ Infrastructure Capabilities

$\beta_1 =$ Slope coefficients for Infrastructure Capabilities

$x_2 =$ Vulnerabilities

$\beta_2 =$ Slope coefficients for Vulnerabilities

$x_3 =$ Authentication Mechanisms

$\beta_3 =$ Slope coefficients for Authentication Mechanisms

$x_4 =$ Information Security Policy

$\beta_4 =$ Slope coefficients for Information Security Policy

$x_5 =$ Training

$\beta_5 =$ Slope coefficients for Training

In this multiple regression analysis, the slope coefficients depict the strength of each of the compliance measures with regard to SMEs Cyber security. To facilitate the prediction of the outcome of the SMEs Cyber security compliance posture, the mathematical model in eq. (2) above was built. Table 4.11 presents the results of this modeling. As shown in Table 4.11, the values in the Sig. column (p-values) are all below the threshold value of 0.05. It is evident that vulnerabilities, authentication mechanisms and training, all have p-values of 0.000. On the other hand,

Infrastructure Capabilities and Information Security Policy have p values greater than 0.05. Consequently, the regression test for SMEs cyber security compliance

Table 4.11: Multiple Linear Regression

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.190	.035		-4.895	.000
	Infrastructure Capabilities	.201	.025	.234	8.042	.03
	Vulnerabilities	.180	.027	.197	6.592	.000
	Authentication Mechanisms	.204	.033	.206	6.183	.000
	Information Security Policy	.179	.025	.198	7.271	.01
	Training	.109	.020	.105	5.345	.000

against Vulnerabilities, Authentication Mechanisms and Training is significant. As such, there is strong relationship between each of the variables and the overall SMEs cyber security compliance.

In Table 4.11, column B gives the slope coefficients of each of the independent variables. Using these coefficients in eq. (2) yields the following:

$$Y = 0.201x_1 + 0.18x_2 + 0.204x_3 + 0.179x_4 + 0.109x_5 + 0.168x_6 + 0.094x_7 - 0.170.19 \quad \text{eq. (3)}$$

Based on eq. (3), the coefficient of 0.180 implies that there is a strong positive relationship between *vulnerabilities* and SMEs cyber security compliance. Similarly, the coefficients of 0.204, and 0.109 indicate strong relationships between SMEs cyber security compliance and Authentication Mechanisms, and *Training* respectively. Figure 4.2 presents the research model for SMEs Cyber security compliance.

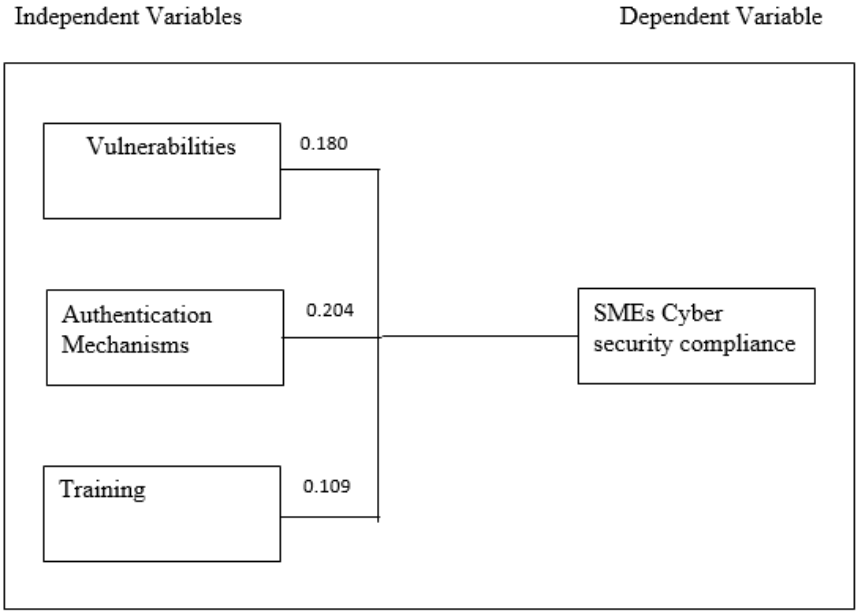


Figure 4.2: Research model for SMEs Cyber security compliance (Researcher, 2024)

To evaluate the effectiveness and reliability of the statistical model in eq. (3) above, Table 4.12 presents the model summary. Basically, it illustrates the performance of the fitted mathematical model in eq. (3) above in terms of key metrics such as R, R-squared value and adjusted R-squared. It also provides a concise overview of the statistical model's fit to the data.

Table 4.12 Independence of Observation (Researcher, 2024)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.980[a]	.960	.960	.101	1.022

a. Predictors: (Constant), Outdated software

b. Dependent Variable: Threats faced

R is the strength of the correlation between our two variables. In our example, there is a very strong correlation of 0.980 between our Outdated Software and Threats Faced. Note that the value of R will always be positive, even when the correlation between the two variables is negative.

R Square tells us how much of the variance in the dependent variable is explained by the independent variable. The value of .960 tells us that 96% of the variance in Outdated Software is explained by threats faced.

Adjusted R Square adjusts R Square on the basis of our sample size. In our example, the Adjusted R Square of .960 is very similar to the R Square of .960. Next, we check the Sig. value in the ANOVA table to determine whether our regression model predicts the dependent variable better than we would expect by chance. Our Sig. value of < .0001 is less than .05, indicating that our regression model is not significant hence the reason of dropping the two variables.

Table 4.13 Anova (Researcher, 2024)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	23.510	1	23.510	2304.000	.000[b]
	Residual	.980	96	.010		
	Total	24.490	97			

a. Dependent Variable: Threats faced

b. Predictors: (Constant), Outdated software

4.1.12 Research model

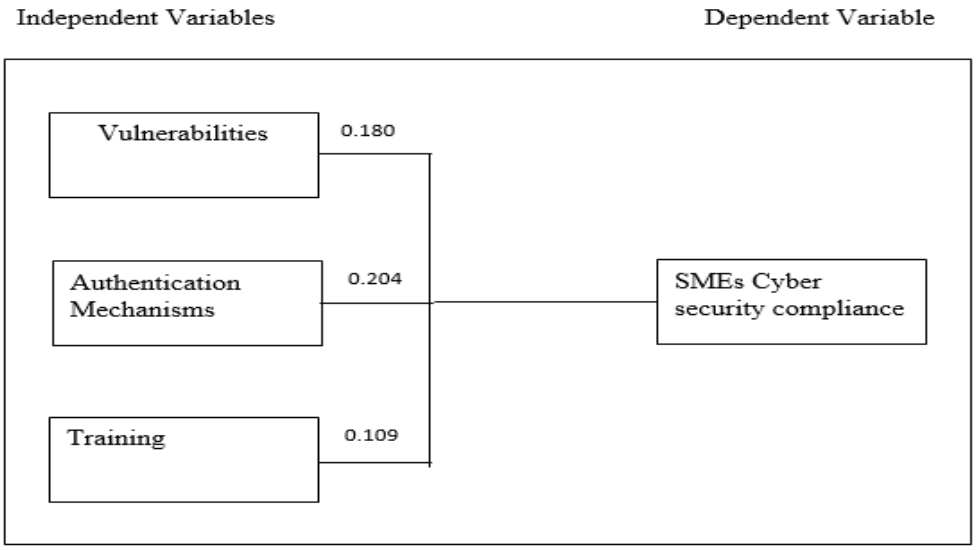


Figure 4.11: Research model (Researcher, 2024)

The research findings clearly show that Vulnerabilities, Authentication mechanisms and user training positively predict Cyber security in Small Medium Enterprises as shown in Figure 4.1.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter summarizes what was stated in the previous chapters. The overall objective of this study is to develop a comprehensive model to mitigate cyber security threats in Small Medium Enterprises in Kenya, strategies, challenges and best practices. It is great to see how this model has been developed and applied in a number of Small Medium Enterprises to see how it can benefit them. Basically, this chapter presents the new findings and information gathered through the research.

5.2 Summary

This chapter highlights the findings of the research, motivated by the research goals and questions. From the questionnaires distributed to employees, respondents were able to provide valuable responses that were analyzed and included in the study. Research shows that employees are not properly trained in security principles, there are limits on data and information available to employees and companies do not have adequate security measures in place in case they could be breached.

Without measures in place, companies will not be able to create a safety culture that can build business and consumer trust. The second objective is to determine whether the SME has a dedicated team to manage cyber security aspects. According to the questionnaire, the majority disagreed on the existence of a response team that could be responsible in case of an attack. This proves that the company may be at high risk of being attacked, especially now that most employees have to come to work using their own devices.

According to an employee, because most people are working from home now, cyber attackers will take advantage of this time to attack. 47% of people working from home fall victim to phishing scams. The leaders promised to look into the matter.

The third goal was to propose a security model. The research question is: does your company have a security model? 98 of those surveyed responded that none of them had this device and that in the event of a serious attack; they would have no choice but to shut down their systems because recovery will not be possible. Therefore, the cyber security model improved company performance by improving working conditions and company security and was thus positively impacted by cyber security.

Finally, the final research question and goal is to test the model. The researcher chose three companies in Nairobi because they were close to the researcher, and they discovered that companies can now receive alert reports when a cyber-security incident occurs as well as when it occurs out and the areas where the violations were committed

The study looked for to distinguish the key challenges of cyber security hazard administration being confronted by ICT Small Medium Enterprises in Nairobi and to create a satisfactory system for cyber security hazard administration to move forward their cyber security status. The inquiry about embracing a clear plan with a target population of 190 Small Medium Enterprises, from which a test measure of 98 respondents was chosen.

The respondents were recognized through non-probability examining within the shape of arbitrary examining. The collection of information was conducted through the use of surveys and, from there on, analyzed through SPSS adaptation 26 so as to be able to draw conclusions. In to determine the connections that existed between the free factors and the subordinate variable, a relapse investigation was utilized. This too encouraged the test of speculations. In approving the in general demonstration, ANOVA was utilized.

The study found that policies in place to educate employees on cyber security had a sum of 7.8 which was low and in order for the threats to be mitigated it needed to increase, the other policies mentioning the companies having designated response team as well as processes used for determining regular evaluation of the framework had an output of 0 indicating the importance of having a model in place

so as it can be used by the organization.

5.3 Vulnerabilities faced by Small and Medium Enterprises

The study found that the organizational cyber security arrangement had not been set up and communicated viably within the ICT Small Medium Enterprises. In understanding how these come about, Mayer (2020) states that a few nations, such as Rwanda, have created a national cyber security arrangement, but there are no particular arrangements tending to particular sorts of Small Medium Enterprises. These arrangements are required to raise awareness around data security and enable workers to meet cyber security needs. Be that as it may, physical gadgets and frameworks inside the organization are inventoried, as well as hypothesized by Vadiveloo et al. (2016).

Having outdated software was a major issue which was affecting Small Medium Enterprises; as a result of this it was easier for hackers to gain access in their systems. A high number of employees were not educated on the importance of cyber security as well as the basics of knowing when they were being sent spam messages which could be having hidden malware which when launched could bring the entire system down.

Authentication Mechanism used in mitigating threats and vulnerabilities faced by Small and Medium Enterprises. The study found that the respondents concurred that the assurance viewpoint was a critical area in cyber security hazard administration. The ranges distinguished in assurance incorporate the issuing of characters and qualifications, administration of physical access to resources, occurrence reaction, confirmation, denial, and reviewing for authorized gadgets, clients, and forms. Almeida et al. (2018) concur that security arrangements and strategies must ensure data resources.

The data security arrangements must be connected across all regions of the institution, and Small Medium Enterprises also have to actualize these security approaches, which may jeopardize their whole commerce and, subsequently, their operational and budgetary practicality.

The study found that the authentication mechanism had a mean of 1.4 making it important to increase the mean so as to ensure that the company is well.

From the study, we could clearly note that companies had not conducted a formal assessment to identify threats and vulnerabilities. This is very dangerous since

some of the employees carried their BYOD devices which might have been affected or affected and can spread to the company infrastructure when connected via Wi-Fi, flash disk or Bluetooth. It was also seen that log data was never collected and analyzed to detect and respond to security incidents which mightcome in handy while assessing data breaches so as to roll back when the first breach started.

5.4 Training

The study found that identified events are analyzed to understand assault targets in ICT Small Medium Enterprises, occurrence caution limits are set up, and the organization is checked to identify potential cyber security occasions. These discoveries are comparable to those of Deloitte (2015), whose organizationis required to create and perform appraisals on the adequacy of the inside cyber- risk controls created and ensure that the qualified personnel can be able to discover them.

Discovery empowers opportune revelation of cyber security occasions such as irregularities and occasions; security ceaseless checking; and location forms. The study found that there was a mean of .0 showcasing training to be implemented making it highly relevant when coming up with a cyber-security model in mitigating threats in Small Medium Enterprises in Nairobi, Kenya.

From the above study, since each Small Medium Enterprises has unique features as well as the services rendered, the Model implemented will have features from NIST Model, COBIT, SOC 2 and SMALL MEDIUM ENTERPRISESEC. The researcher was able to drop two independent variables since they did not satisfy the regression test model when compelling the final model.

5.5 Conclusion from the above summary

The following can be concluded from this study. The following can be concluded from this study:

Human factor are the main source of data breaches and in order to reduce them, training should be done time to time to ensure that your staff are well equipped with knowledge on how to protect themselves as well as the company resources.

It is important for regular updates of software to be made as well as buying from credible companies. This will ensure that minimal entries by the hackers will be

there in order as to gain access to your software

When people are allowed to come with BYOD, there should be special segment in the Wi-Fi for such people as well as for guests, this will be handy when there are hacking attempts as this will be easier for the it personnel to brute force a see areas and time when the breach started

For Small Medium Enterprises it is a very important for them to have a Model which will be used before, during and after an attack so as to know how tomitigate, solve or sought out a breach when it happens.

5.6 Recommendation for implementation

Small Medium Enterprises should stop assuming that cyber security only affects large organization and instead agree to get the resources to protect them. Constant training should be rolled out to the users

Companies should regularly update their software to ensure they are well secured.Researchers should continue doing more research in matters affecting Small Medium Enterprises and not only focus on corporates since they also part of the companies.

REFERENCES

Castro, D. (2018). Preparing Small Business for Cybersecurity Success - Testimony of Daniel Castro Before theSenate Committee on Small Business and Entrepreneurship. Information Technology and Innovation Foundation (ITIF).

Controls, C. (2016). Updates on French Encryption Controls and Their Interplay with EU RegulationsIntroduction. Internet Security Threat Report. (2016). 21(April).

Information Security Forum Limited. (2011). The 2011 Standard of Good Practice for Information Security.

June, 292. https://www.uninett.no/webfm_send/730

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats andpractices in small businesses. Information Systems Management, 22(2), 7–19. https://doi.org/10.1201/1078/45099.22.2.20050301/87273.2

Pirotti, A. (2007). Preface. ISSE/SECURE 2007 - Securing Electronic Business Processes:

Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, January.https://doi.org/10.1007/978-3-8348-9418-2

Polkowski, Z. (2017). It Security Management in Small and Medium Enterprises. Buletin Ştiinţific: UniversitateaDin Piteşti. Seria Ştiinţe Economice, 16(3), 134–148.

Renaud, K. (2016). How smaller businesses struggle with security advice. Computer Fraud & Security, 2016(8),10–18. https://doi.org/https://doi.org/10.1016/S1361-3723(16)30062-8

The Australian Small Business and Family Enterprise Ombudsman. (2017). Cyber Security: The Small BusinessBest Practice Guide Cyber Security: A Small Business Best Practice Guide.

Pirotti, A. (2007). Preface. ISSE/SECURE 2007 - Securing Electronic Business Processes:

Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, January.https://doi.org/10.1007/978-3-8348-9418-2

Research, T. J. & M. L. G. C. for A. (2016). Cyber Risk for Small and Medium-Sized Enterprises. University ofConnecticut, Aug. http://goldensoncenter.uconn.edu/wp-content/uploads/sites/912/2014/09/CyberRiskDraftReport-9-27-2016-Final-without-comments.pdf

Serianu. (2017). Demystifying Africa ’ s Cyber Security Poverty Line. Annual Cybersecurity Report.

The Australian Small Business and Family Enterprise Ombudsman. (2017). Cyber Security: The Small BusinessBest Practice Guide Cyber Security: A Small Business Best Practice Guide.

United Nations Interregional Crime and Justice Research Institute (UNICRI). (2015). Guidelines for IT security in Small Medium Enterprises. 9. www.unicri.it

Valli, C., Martinus, I., & Johnstone, M. (2014). Small to Medium Enterprise Cyber Security Awareness: an initialsurvey of Western Australian Business. Proceedings of the International Conference on Security and Management (SAM), 2020(July), 1.

Advisory, B. (2024, Jan 8). How to Implement an Information Security Program in 9 Steps. Retrieved from Barr Advisory: https://www.barradvisory.com/resource/how-to-implement-an-information-security-program-in-9-steps-2/

Advisory, B. (n.d.). Barr Advisory. Retrieved from https://www.barradvisory.com/resource/how-to-implement- an-information-security-program-in-9-steps-2/

Alahmari A, D. B. (2020). 2020 International Conference on Cyber Situational Awareness, Data Analytics andAssessment, Cyber SA 2020.

DataGuard. (2023). https://www.dataguard.co.uk/blog/steps-to-cyber-security/. Retrieved from DataGuard.

Directory, K. B. (2023). Retrieved from https://www.kenyabizlist.com/

frinking, N. C. (2023). Assessing Cyber Security: A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks. Retrieved from Nicolas CastellonProfile image of Jacques MukenaJacques MukenaProfile imageof erik frinkingerik frinking

Fujitsu. (2023). https://www.fujitsu-general.com/us/resources/pdf/support/downloads/installation-instructions/pdf-92-20521-106-fh-tps.pdf. Retrieved from Fujitsu.

Guidance. (2021, May 11). 10 Steps to Cyber Security. Retrieved from National Cyber Security Center:https://www.ncsc.gov.uk/collection/10-steps

Heimdal. (2023). Application Whitelisting Concepts: Definition, Types, Implementation and Best Practices. Retrieved from https://heimdalsecurity.com/blog/application-whitelisting/

Imperva. (2024). Retrieved from https://www.imperva.com/learn/data-security/soc-2-

compliance/

K, S. S. (2020). Using an extended Technology Acceptance Model to understand students' use of e-learningduring Covid-19: Indonesian sport science education context.

Kasper Hornbæk, M. H. (2017). Technology Acceptance and User Experience: A Review of the ExperientialComponent in HCI. ACM Transactions on Computer-Human Interaction .

Lyytinen†, E. M.-O. (2003). Why organizations adopt information . Info Systems J .

Marie-Laurence Caron-Fasan, N. L. (2020). Adoption of enterprise social networking: Revisiting the IT innovation adoption model of Hameed et al. The Journal of Engineering and Technology Management.

McCluskey, S. (2017). Australian Small Business and Family Business Ombudsman, 2017. AustarlinGovernment .

NDNB. (2024). Comprehensive Audit details you should know. Retrieved from https://socreports.com/audit-overview/what-is-soc-2

Norman. (2023). https://preyproject.com/blog/how-to-implement-a-successful-cybersecurity-plan. Cybersec Essentials. Retrieved from https://preyproject.com/blog/how-to-implement-a-successful-cybersecurity-plan.

Onelogin. (2024). Modern Multi-Factor Authentication. Retrieved from https://www.onelogin.com/product/multi-factor-authentication

Pavlou, P. A. (2016). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with theTechnology Acceptance Model. International Journal of Electronic Commerce .

Rebecca Schnall, M. R.-D. (2016). A user-centered model for designing consumer mobile health.https://dl.acm.org/toc/jobi/2016/60/C.

Rogers, E. M. (2009). Diffusion of Innovations. University of Illinois at Urbana-Champaign's Academy forEntrepreneurial Leadership Historical Research Reference in Entrepreneurship.

Stevens, A. (2024). https://www.6clicks.com/resources/answers/what-is-the-10-steps-to-cyber-security.
Retrieved from 6clicks.

Xiaoyun Wang, K. S. (2012). Advances in Cryptology. Retrieved from

https://link.springer.com/book/10.1007/978-3-642-34961-4

Xiaoyun Wang, K. S. (2012). Advances in Cryptology.

Younghwa Lee, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoreticalperspective. Information & Management.

Zmud, R. B. (2022). Information Technology Implementation Research: A Technological Diffusion Approach.

Management Science.

APPENDICES 1: QUESTIONNAIRE

DEVELOPING A MODEL FOR THE PREVENTION OF CYBER SECURITY THREATS IN SMALL AND MEDIUM ENTERPRISES

PART 1: GENERAL INFORMATION

What is your gender?

- ◯ Male
- ◯ Female
- ◯ Prefer not to say

What is your age bracket?

- ◯ 20 - 35
- ◯ 36 - 45
- ◯ Above 46

PART 2: THREATS AND VULNERABILITIES FACED BY SMALL AND MEDIUM ENTERPRISES

Are there any cloud-based services or applications used?

◯ Yes ◯ No

Are there any legacy systems or outdated software in use?

◯ Yes ◯ No ◯ Maybe

Are there any specific policies or guidelines in place to educate employees about cyber security? *

- ◯ Yes
- ◯ No

Are strong passwords and multi-factor authentication enforced?

◯ Yes ◯ No

◯ To some extent

Is there a backup strategy in place to protect critical data?

◯ Yes ◯ No

Does the SME engage with third-party vendors or partners who may have access to sensitive data or systems?

◯ Yes ◯ No

PART 3: TOOLS USED IN MITIGATING THREATS AND VULNERABILITIES FACED BY SMALL AND MEDIUM ENTERPRISES

Has the SME conducted a formal assessment to identify threats and vulnerabilities?

◯ Yes ◯ No

10 If yes, please provide details about the assessment process and any findings or recommendations.

_____

_____

_____

_____

Does your company have antivirus or endpoint protection software installed on all devices

◯ Yes ◯ No

Are there encryption measures in place to protect sensitive data at rest?

◯ Yes ◯ No

Does your company utilize access control mechanisms (e.g., role-based access control) to restrict user permissions?

◯ Yes ◯ No

Is log data collected and analyzed to detect and respond to security incidents?

◯ Yes ◯ No

Does the SME have a backup strategy to protect critical data?

◯ Yes ◯ No

Are backups regularly performed and tested for data restoration?

◯ Yes ◯ No

Is there a disaster recovery plan to ensure business continuity in the event of a cyber-incident?

◯ Yes ◯ No

PART 4: HOW EFFECTIVE WILL A MODEL WHICH WILL BE USED TO PREVENT CYBER SECURITY THREATS IN SMALL AND MEDIUM ENTERPRISES

Has your organization implemented a cyber-security Model?

◯ Yes ◯ No

If yes, please provide details about the Model used.

Are risks prioritized based on their potential impact on the organization?

◯ Yes ◯ No

Is there a designated incident response team responsible for handling cyber security incidents? *

◯ Yes ◯ No

Is there a process for regularly evaluating and improving the effectiveness of the Model?

◯ Yes ◯ No

Thank you for filling this questionnaire.

APPENDICES 2: Research Permits

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 284319

Date of Issue: 22/July/2024

RESEARCH LICENSE

This is to Certify that Miss. Rose Waithera Kiragu of Africa Nazarene University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: DEVELOPING AN INCLUSIVE PROTOTYPE AND FRAMWORK FOR RUNNING AND PREVENTING CYBER SECURITY THREATS IN SMALL AND MEDIUM BUSINESSES IN NAIROBI, KENYA for the period ending : 22/July/2025.

License No: NACOSTI/P/24/38211

284319

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

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

See overleaf for conditions

APPENDICES 3: Research Approvals and Letters

AFRICA NAZARENE
UNIVERSITY

3rd April 2023

To whom it may concern,

Dear Sir/ Madam,

RE: PROPOSAL APPROVAL FOR ROSE WAITHERA KIRAGU (19J03DMIT012)

The above named is a Master of Science in Applied Information Technology student at Africa Nazarene University. This is to confirm that her research proposal titled "**A FRAMEWORK FOR THE PREVENTION OF CYBER SECURITY THREATS IN SMALL AND MEDIUM BUSINESSES**" has been approved for conduct of research, subject to obtaining other permissions and/or clearances that may be required beforehand.

Any support and/or assistance accorded to her will be highly appreciated.

Please feel free to contact me via email on hodcit@anu.ac.ke in case of any questions.

Sincerely,

Edward Ombui, PhD.
Head of Department, Computer and Information Technology

APPENDICES 4: Map of Study Area