CYBERSECURITY ASSESSMENT MODEL FOR SMALL AND MEDIUM ENTERPRISES (SMEs) E-COMMERCE IN KENYA

BY:

KIBET SANG

A RESEARCH DISSERTATION SUBMITTED IN PARTIAL FULFILMENT FOR

THE REQUIREMENTS FOR THE AWARD OF A DEGREE IN MASTER OF SCIENCE IN INFORMATION SYSTEMS MANAGEMENT IN THE SCHOOL OF TECHNOLOGY AT KCA UNIVERSITY.

SEPTEMBER, 2023

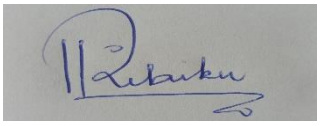
DECLARATION

I declare that this dissertation is a result my original work and has not been previously published or submitted for award of a degree. I also declare that this dissertation contains no material written or published by other people except where due reference is made, and authors duly acknowledged.

STUDENT NAME: KIBET SANG **REG. NO: 21/02300**

SIGN: **DATE: 12TH SEPTEMBER 2023**

I do hereby confirm that I have examined the master's dissertation of **KIBET SANG,** and have approved it for examination.

SIGN:  **DATE: 12TH SEPTEMBER 2023**

DR. KIBUKU RACHAEL

RESEARCH SUPERVISOR

ABSTRACT

In Kenya, there has been a remarkable surge in the adoption of e-Commerce among Small and Medium Enterprises (SMEs), especially in the aftermath of the COVID-19 pandemic. This has seen several online stores developed and launched for Business-to-Consumer(B2C) e-Commerce. However, the rise of e-Commerce platforms has also led to an increased number of cyber-attacks and data breaches, leading to financial losses, damage to reputation, and decreased market share for SMEs with no cybersecurity strategies. This phenomenon is primarily caused by a lack of cybersecurity assessment models that are adapted to the specific demands of SMEs e-Commerce platforms. This study sought to assess e-Commerce's cybersecurity level and maturity for SMEs in Kenya by developing assessment model.

This study reviewed some theoretical framework, standards, models, and empirical study to guide the development of the model. A tailored cybersecurity assessment model was developed specifically for SMEs operating in the e-Commerce sector in Kenya. The study assessed e-Commerce cybersecurity maturity level by using mixed methods approach with a focus on experimental research design, and determined the most common cyberattacks in relation to e-Commerce operations.

The assessment included various metrics such as access control mechanisms, software, data security, authorization and authentication, and network, and was rated quantitatively on a scale of 1-100 with critical, moderate, and highly secured as qualitative output of the model. The study involved 40 SMEs, all of whom responded to a semi structured questionnaire, and 36 agreed to have their e-Commerce platforms assessed using the model developed. Out of 36 e-Commerce assessed, 34 were found to be most vulnerable to cyberattacks, with a critical rating and assessment falling below 50 points, while only two were considered moderate or secure for online operations. The study concluded that SMEs must implement robust cybersecurity measures and standards, including access controls, authentication and authorization, data security, software security and network security since the study discovered that all the variables in the model are contributing to overall security. The study recommends specific policy formulation on cybersecurity to control deployment of e-Commerce. The study further recommends a study on user behaviour and online trends in managing e-Commerce cybersecurity.

KEYWORDS: ***SMEs, B2C, Cybersecurity,*** **Cyber-Attacks**, ***Cybersecurity Assessment Model.***

ACKNOWLEDGEMENTS

I want to thank everyone who played a role in making this dissertation a success. I thank God for His divine guidance and for providing me with the strength and perseverance to complete this dissertation.

I extend appreciation to my supervisor, Dr. Kibuku Rachael, for dedicating her time and expertise to guide me through every step of this research, including long meetings. Her invaluable insights, constructive detailed feedback, and unwavering support were instrumental in shaping the outcome of this thesis.

I would also like to give thanks to my parents for their constant support and encouragement. My dad, Philip A. Kobel, and mum Eunice C. Kobel, your unwavering love and support have constantly motivated and inspired me to keep going. Thank you for always being there for me and for believing in me, even when the going got tough.

I extend my gratitude to all the respondents who participated in this research. Your willingness to share your experiences and insights was crucial in shaping the outcome of this study. I am grateful for your time and contributions.

TABLE OF CONTENTS

PAGE

DEDICATION

I dedicate this dissertation to my parents Philip A. Kobel, and Eunice C. Kobel, for their unwavering support, encouragement, and daily prayers.

LIST OF TABLES

TABLE **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

ACRONYMS AND ABBREVIATIONS

B2C	Business to Consumer
BeEF	Browser Exploitation Framework
CMMC	Cybersecurity Maturity Model Certification
CSF	Cybersecurity Framework
CIA	Confidentiality, Integrity, and Availability
CIRT	Computer Incident Response Team
CMS	Content Management Systems
DDoS	Distributed Denial of Service
DoS	Denial of Service
GVM	Greenbone Vulnerability Management
HSTS	HTTP Strict Transport Security
ICS	Index of Cyber Security
ICS	Index of Cyber Security
ITU	International Telecommunication Union
KE-CIRT/CC	National Kenya Computer Incident Response Team – Coordination Centre
KNBS	Kenya National Bureau of Statistics

NIST	National Institute of Standards and Technology
NCSI	National Cyber Security Index
NIST	National Institute of Standards and Technology
OSINT	Open-Source Intelligence
PCIDSS	Payment Card Industry Data Security Standard
QoD	Quality of Detection
QSA	Qualified Security Assessor
SAQ	Self-Assessment Questionnaire
SIEM	Security Information and Event Management
SME	Small and Medium Enterprises
SMECRA	SME Cyber Risk Assessment
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UNCTAD	United Nations Conference on Trade and Development
XSS	Cross-site scripting
2FA	Two Factor Authentication
VPS	Virtual Private Server

DEFINITION OF TERMS

Small and Medium-Sized Enterprise (**SME**): This is a business classification that is typically applied to companies with fewer than 500 employees and annual revenues that fall below a certain defined threshold and employee number is based on their turnover (Whah & Shiang, 2018).

Business-to-Consumer(B2C): This is a retail-based online business, it is a business model where companies and SMEs sell products or services directly to individual consumers. Online businesses interact directly with customers, offering a wide range of products and services through online stores (Tamplin, 2023).

Cybersecurity is the process of protecting and securing cyberspace that is; networks, computers, servers, mobile devices, and data from cyberattacks, theft, and damage (Kelley, 2023; Kaspersky, 2023; Arnold and Jr, 2022b; Sulistyowati et al., 2020).

Cyber-attacks refer to malicious activities or actions conducted by individuals or groups with the intent to compromise, disrupt, or damage computer systems, networks, or digital devices (Kaspersky, 2023).

Cybersecurity model is a framework that outlines strategies and technologies to protect computer systems, networks, and data from unauthorized access and threats. It includes measures like risk assessment, threat detection, incident response, standards compliance, and ongoing monitoring (Simplilearn, 2022b).

CHAPTER 1: INTRODUCTION

1.1 Background of Study

The main goal of cybersecurity is to achieve the Confidentiality, Integrity, and Availability (CIA) triad for data and services. Cybersecurity secures cyberspace, the environment in which internet-connected devices communicate (Kelley, 2023; Hijji & Alam, 2022; Sulistyowati et al., 2020). Cybersecurity is critical in every organization, whether government or private, because they have processed and stored massive amounts of data over time (Arnold & Jr, 2022b). Cyberspace protection can take several forms, including controlled access to data and systems, policies, monitoring for intrusion, raising awareness, and network protections such as the use of firewalls.

E-Commerce is buying and selling goods or services over the internet and paying for the goods and services to complete and close the transactions (Zande, 2022; Jain et al., 2021; Išoraitė & Miniotienė, 2018). The e-Commerce process involves selling physical products and services online, as well as transacting the goods and services.

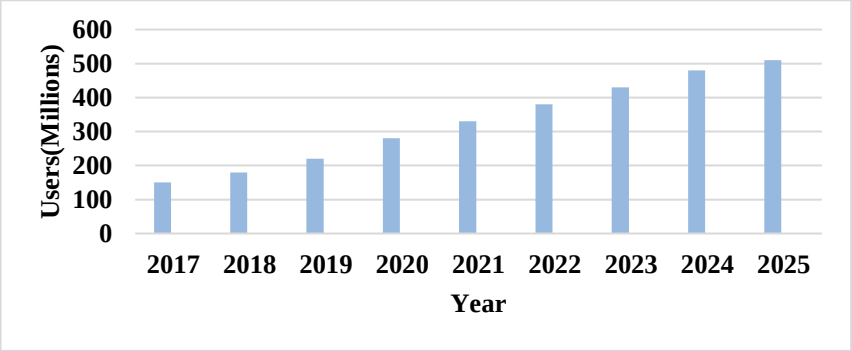
The internet saw a rapid expansion in the 1990s and this resulted in a substantial number of domain name registrations. However, this growth brought about security concerns on certain online platforms, this was addressed by Netscape which developed Secure Socket Layers (SSL) encryption certificates. These certificates played a crucial role in establishing trust in websites and ensuring that internet users felt more secure while accessing online content. The first secure online transaction occurred in 1994, when Dan Kohn founded an e-Commerce platform called NetMarket and used the platform to sell a Sting compact disc to a friend, Kohn, who in turn paid $ 12.48 plus shipping, payment was made by sending credit card information via data encryption software

(Rosa, 2020). There was major e-Commerce development in 1990s, Amazon's revenues had a significate growth from $15.7 million in 1996 to $610 million in 1998 (Tamplin, 2023). The rise in business-to-consumer (B2C) online sales did present some challenges for business running a traditional form of businesses. The traditional businesses models of physical stores are dramatically reducing as more customers turn to e-Commerce, the online stores offer convenience in terms of time and delivery of goods. The Business-to-Business (B2B) model is another business that involves businesses engaging in the exchange of products or services with other businesses. The B2B model has also experienced a notable increase in popularity, with the global B2B e-Commerce market reaching a valuation of $7,907.07 billion in 2022. Projections indicate that this market will continue to expand, with an anticipated growth rate of 20.2% from 2023 to 2030 (Tamplin, 2023)

The case of NetMarket online purchase platform is a type of Business-to-Consumer(B2C) e-Commerce model, which is a business model that involves selling goods and services between online B2C via the World Wide Web (Zande, 2022). The growth of e-Commerce B2C businesses in Kenya has been impressive and commendable. In recent years, Kenya has seen a significant increase in the rate of e-Commerce adoption. Kenya was ranked at position 88 globally among the countries with the fastest growing e-Commerce economies globally and fourth in Sub-Saharan Africa in the B2C Commerce Index (United Nations Conference on Trade and Development (UNCTAD),2020). According to International Trade Administration (2021) predictions, the e-Commerce user base will exceed 500 million in Africa by 2025 with consistent compound annual growth rate of 17%. Kenya’s e-Commerce industry is projected to generate $3,292.00m in 2023, with annually growth rate of 6.63% with e-Commerce users expected to hit 38 million users by

2027(Statista, 2021). Figure 1 presents an overview of the progression of e-Commerce users throughout the years, along with a projected estimate of the number of users anticipated by the year 2025.

FIGURE 1: e-Commerce Penetration in Africa (Source ITA,2021)



The e-Commerce digital revenue in Kenya generated in 2020 was US $1.1 billion, with an annual growth rate of 16.4% projected by 2025 (Statista, 2020). The growth of e-Commerce has contributed to cyberspace in Kenya, with 143,040,599 cyber threat events detected in July - September 2021, a 268.883% increase from the previous reported figure of 38,776,699 in April - June 2021, (National Computer Incident Response Team National KE-CIRT/CC, 2021).

Phishing attacks campaign targeted 200 million Microsoft 365 users globally across financial, healthcare insurance, manufacturing, utilities, and telecom sectors. In addition, there was an increase in malicious phishing attacks targeting online shoppers in the form of "offers" and primarily during the holiday shopping season, to trick unsuspecting online shoppers. The fraudsters used spoofed email addresses and shared a link to a newly registered domain that was spoofing a legitimate website (Sheridan, 2020). National KE-CIRT/CC (2020), anticipated an increase in

fraud targeting e-Commerce platforms, and the National KECIRT/CC undertook user awareness on fraud in online platforms, primarily through information gathering such as user credentials and credit card details. Web application attacks have increased dramatically in Kenya, with 2,564,173 detected in April-June 2021, and 478,123 detected in the July -September 2021 period. Web attacks primarily exploited vulnerabilities such as web application configuration errors in the program code, outdated software plugins, and a lack of technical personnel to secure web applications (Kaur & Kaur, 2016). Web attacks primarily occurred in the form of code injection attacks on WordPress sites via the Welcart plugin e-Commerce vulnerability. The vulnerable plugin allowed cyber criminals to retrieve information via SQL injection, as well as unpatched or updated cPanel, which saw Two-Factor Authentication(2FA) bypass and took control of a web application on a shared hosting environment. In a survey conducted by Kaspersky (2022) in the middle of the year 2022, there were 100,192 instances of cyber-attacks involving financial phishing aimed at organizations in Kenya. This marked a significant increase of 201% compared to the beginning of the year. The primary targets of these attacks were e-Commerce websites, which accounted for 58% of the total attacks. Banks and payment systems were also targeted, each accounting for 21% of the attacks.

Client-server architecture is the foundation of most e-Commerce platforms. Where a user device/s is the client, users use the graphical user interface to request services from the server; the server processes the user request and sends the response to the client in resources or services. Since operations occur in cyberspace, security is not an option (Terra, 2023). The CIA triad must be guaranteed by the operations. The e-Commerce platform should be secured at all costs, and an awareness campaign should ensure users know the precautions they should take when shopping online. The e-Commerce has simplified shopping, reduced the cost of running a physical store, and

provided greater convenience to customers. To maintain digital trust, merchants operating online stores should ensure secure data sharing and storage (Ferreira, 2022).

The cybersecurity assessment model can be framed as a multivariable evaluation and analysis of risk of the cybersecurity threats to web systems. The model evaluates security implementation of the systems, by scanning for vulnerability, testing, risk assessments, and compliance to specific standards and regulations. The Cybersecurity Framework (CSF) is one of the used models in assessing compliance to standards, the model was as a result of a research by National Institute of Standards and Technology (NIST) in 2014. The CSF details a set of guidelines, procedures and standards that an organisation can use to improve the cybersecurity implementation of the system. The ISO/IEC 27001 standard added to the list of models and standards used to audit the security of the information technology environment. The standard also guides the development of models for assessing a unique systems cybersecurity implementation, it gives the base factors for consideration in framing the variables of any model. Payment Card Industry Data Security Standard (PCI DSS) provided a list of standards that organizations that transact with credit card payments must be comply to in order to operate secure transactions.

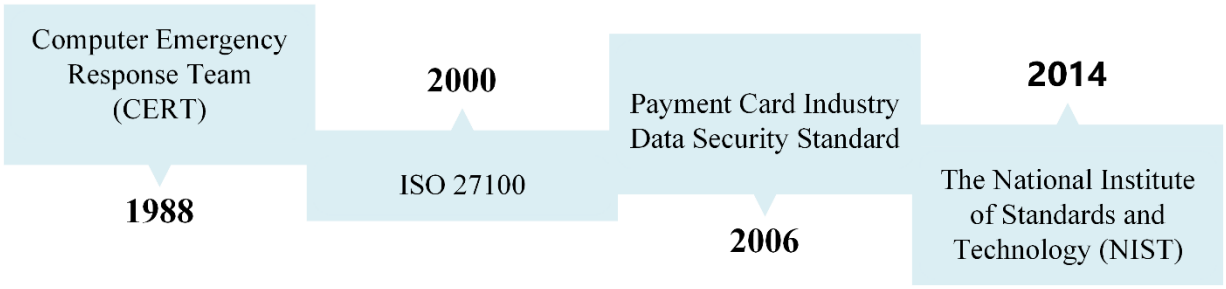
1.2 History of Cybersecurity Assessment Models

The need for cybersecurity assessment rose in the year 1970s and 1980s due to the high growth of technology advancement and rise of cyberthreats in cyberspace. The first model of such kind was the Computer Emergency Response Team (CERT) which was a product of Carnegie Mellon University ‘s research in the year 1988. The CERT Coordination Centre developed a set of incident response strategies and controls and also procedures on the vulnerability disclosure, the model

became a basis of the cybersecurity implementation standards. Several other cybersecurity evaluation models, frameworks and standards were developed in the 1990s. The International Organization for Standardization (ISO) accepted the British Standards Institution (BS 7799) standard for cybersecurity management in ISO 17799 in 2000, which was eventually replaced by ISO 27001. The National Institute of Standards and Technology (NIST) announced its first cybersecurity framework in 2014, which has since been modified multiple times, most recently in 2023 Version 2.0.

In the aftermath of the 2000s, cybersecurity assessment models got more thorough, covering a broader spectrum of cybersecurity challenges. The Payment Card Industry Security Standards Council (PCI SSC) created the Payment Card Industry Data Security Standard (PCI DSS) in 2006 to assist protect credit card information. The Cloud Security Alliance (CSA) developed a matrix for Cloud Controls in 2008 to give a model for analysing the security of cloud computing services. Figure 2 shows the history of various standards and frameworks developed and published over the years.

FIGURE 2: History of Cybersecurity Assessment Models (Source Research)



1.3 Problem Statement

The rise of B2C e-Commerce platforms in Kenya has led to an increase in security risks associated with online transactions, especially for SMEs (Muhati, 2018). SMEs do not have reliable and efficient models and frameworks tailored to their operations, to assess their B2C platforms before deployment, this has seen an increase in cybers attacks on their platforms resulting in data breaches, financial loss, payment fraud, cybercrime, social engineering attacks, damage to reputation, legal suit, industrial espionage, and denial of services among Kenyan SMEs running B2C commerce (Kaspersky, 2022; Muhati, 2018; Mwangi et al., 2017).

The existing models and frameworks have failed to address cybersecurity assessment by SMEs, Mthiyane et al. (2022) study discovered that the Enterprise Risk Management model for system assessment via risk analysis was resource intensive and limited resources hinder SMEs' from implementing it, since it relies on methodological risk analysis and mitigation, Ramadhan & Rose (2022) study discovered that ISO/IEC 27001 standards as a model for assessing the systems security level via system audits, was resource intensive, requires cybersecurity expertise and had privacy concerns which hinders implementation, the model relies on subjective analysis of system

by the auditors. The SMECRA model for evaluating efficiency of cybersecurity strategies, is resource intensive and do not cover the unique needs of SMEs online stores (Armenia et al., 2021). Kravets (2019) study discovered that the Global Cybersecurity Index, Cybersecurity Maturity Model Certification, Index of Cyber Security, National Cyber Security Index adopt subjective assessment techniques in assessing the cybersecurity of the country, rely on limited data due to self-assessment, lack flexibility and standardization, there is no validation, and do not consider SMEs' unique needs in determining their cybersecurity maturity since it focuses on the assessment of the country as a whole and not individual system cybersecurity maturity.

This study aims to address the gap in SMEs' cybersecurity assessment by developing a cybersecurity assessment model that is objective and data-driven, considers SMEs' unique needs, and is flexible, cost-effective, and validated for e-Commerce platforms implemented by SMEs in Kenya.

1.4 Research Objectives

1.4.1 General Objective

The main objective of this research was to develop cybersecurity assessment model for SMEs e-Commerce platforms in Kenya.

1.4.2 Specific Objectives

i. To identify existing cybersecurity assessment models to determine their strengths and limitations.
ii. To identify the key cybersecurity assessment factors that should be considered in developing a cybersecurity assessment model.

iii. To develop a cybersecurity assessment model, using key factors, their attributes, and relationships between them.

iv. To validate the model.

1.5 Research Questions

The main research question for the research will be: "*What key cybersecurity assessment factors should be considered in developing cybersecurity assessment model*?" Specifically, the research will answer the following questions.

i. What are the existing cybersecurity assessment model and how do they compare in terms of their comprehensiveness, efficiency, strengths and limitations, and ease of use?

ii. What are the key cybersecurity assessment factors that should be considered in an assessment model?

iii. How can a conceptual framework be developed for the proposed cybersecurity assessment model, including the factors, their attributes, and relationships between them?

iv. How can the model be validated?

1.6 Scope of the Research

The research focused on the B2C e-Commerce platforms of SMEs in Kenya specifically cosmetics and fashion, general e-Commerce platforms, electronics online store and booking platforms and provided insights and recommendations that can be applied to other similar e-Commerce platforms in Kenya.

1.7 Significance of the Research

This research output will provide significant benefits to a variety of stakeholders, including and not limited to cybersecurity professionals, e-Commerce administrators and developers, academicians, policy makers and decision makers, user of e-Commerce, and governments.

i. The model can provide e-Commerce platforms developers with the standards and guidelines for building secure e-Commerce platforms.
ii. Academicians, and the researchers can use the model to research on the intersection between the e-Commerce and cybersecurity.
iii. The Governments, policy makers and the decision makers will use the output of the model to formulate the policies and regulation to guide the development of the e-Commerce.
iv. Cybersecurity professionals can benefit from the output of the model in determining common vulnerabilities being exploited and providing means of fixing and improving the cybersecurity tools.
v. The data of e-Commerce users will be secure.

1.8 Research Motivation

The study was motivated by a number of factors, the first is the financial losses in form of cyber fraud, resulting from cyber-attacks directed to the e-Commerce. The second motivation was the high rate of data breaches that results in exposure of sensitive information and a number of identity theft in the digital commerce, and the reputational damage. The third motivation was the corporate espionage which arise from data stolen via cyberattacks. The high rate of cyber law, legal

consequences and fines experienced by the SMEs due to violation of the cyber law and due to negligence on e-Commerce cybersecurity implementation also drove the research need.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The increasing reliance on technology and the increasing number of interconnected devices has resulted in an exponential growth in cybersecurity threats and incidents in recent years. The literature review chapter provided an overview of existing cybersecurity assessment models and frameworks, including their features and use cases, as well as their limitations and challenges. This helped understand the state of cybersecurity assessment model and frameworks and identify gaps that needed to be researched and upgraded. Through a comprehensive review of existing literature and research studies, this chapter laid the foundation for developing a new cybersecurity assessment model that addressed the specific needs of Kenya's SMEs. Gaps, limitations, and challenges of existing models and frameworks were identified and addressed in the developed model.

2.2 Theoretical Background

2.2.1 Cybersecurity Frameworks

The cybersecurity frameworks provide strategies and methodologies for assessing the cybersecurity status for various systems. The frameworks rate the cybersecurity implementation using different scale and methods. There are a number of cybersecurity frameworks: -

a) The Global Cybersecurity Index

The Global Cybersecurity Index (GCI) is a model developed by the International Telecommunication Union (ITU) to measure the commitment of governments to cybersecurity on

a global scale (Kravets, 2019). The GCI aims to promote awareness of cybersecurity's importance and highlight the problem's dimensions. The index assesses the cybersecurity development and implementation in a country in five thematic areas, as well as how governments' commitments to raise awareness of the cybersecurity importance and various dimensions of the problem (Kravets, 2019). Bruggemann et al. (2022) discusses the Global Cybersecurity Index as a control and feedback mechanism based on a composite indicator comprised of five itemized indicators referred to as pillars. Each pillar is further divided into sub-indicators, which are used to evaluate the country's level of cybersecurity.

i. Legal measures, these include assessing cybercrime and cybersecurity of laws, regulations, and policies related to cybersecurity in a country.
ii. Technical measures, assesses the level of technical infrastructure and the availability of cybersecurity services through national and sub sectors.
iii. Organizational measures, existence of institutions and organizations responsible for cybersecurity in a country.
iv. Measures of capacity development, assesses the availability of education and training programs related to cybersecurity.
v. Cooperative measures, assesses the level of international cooperation in cybersecurity include assessing partnerships between agencies, businesses, and countries.

The legal measures, technical measures, organizational measures, capacity building and cooperation, are the thematic areas which are graded, and the total grade is obtained by adding all

the grades. Each thematic area has questions and marks; the questions are in the form of an online survey, and the marks assigned to each question are determined by experts from partner organizations; the answers must be accompanied by a supporting document; and the total marks for all the considered questions is 100 units (Kravets, 2019). The GCIv2 methodology employs a binary evaluation system (0,1) to determine whether a specific indicator or element is captured. A three-tiered system was used in 2014: -

a) Existent.
b) Partially developed.
c) Absent.

Table 1 gives a summary of variables and attributes considered in the GCI methodology.

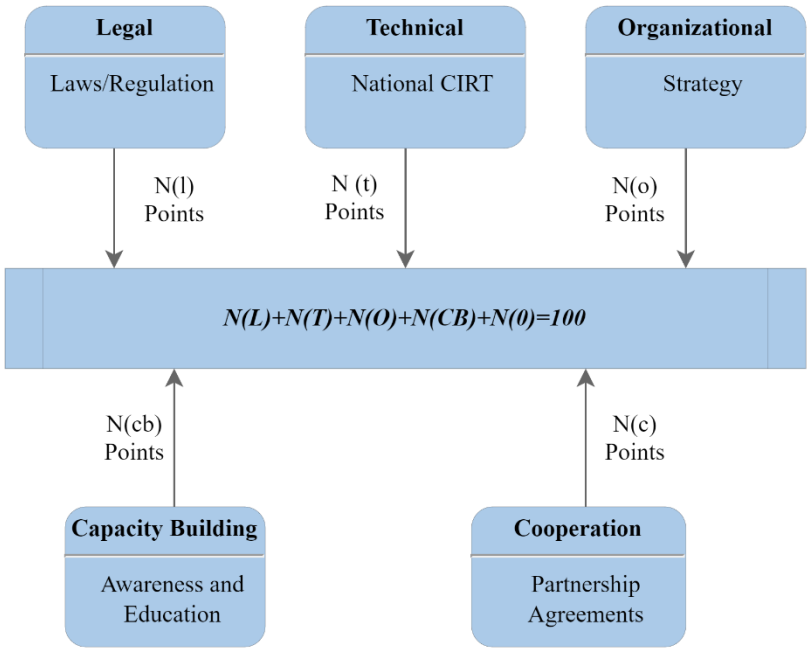
TABLE 1:The Global Cybersecurity Index Methodology (Source: GCI, 2014)

VARIABLES	ATTRIBUTES/INDICATORS
Legal	– Cybercriminals legislations – Substantive Law – Procedural Cybercriminal law – Cybersecurity Regulation
Technical	– National CIRT – Government CIRT – Sectoral CIRT – Standards for Organizations – Standardizations body
Organizational	– Strategy – Responsible Agency – Cybersecurity Metrics
Capacity Building	– Public awareness – Professional training – National education- R&D programs – Incentive mechanisms – Home-grown Industry

VARIABLES	ATTRIBUTES/INDICATORS
Cooperation	– Intra-state cooperation – Multilateral agreements – Public-Private partnerships – Inter-agency partnerships

Figure 3 demonstrate the operation of GCI.

FIGURE 3 : The Global Cybersecurity Index



Limitations of Cybersecurity Index Framework

The cybersecurity index framework has a number of limitations that has made it less effective in assessing the cybersecurity maturity, these limitations include: -

i. Lack of data availability, as some countries may not have the necessary data to be included in the GCI, in addition the GCI relies on self-reported data, which may not always be accurate.
ii. Lack of standardization in the way countries measure and report on cybersecurity, making it difficult to compare the results from different countries.

b) The National Cyber Security Index (NCSI)

The National Cyber Security Index (NCSI) is a cybersecurity assessment model that evaluate the cybersecurity status and implementation in a given country (Kravets, 2019). The model was a research output of the e-Governance Academy Estonia. The model operations are based on techniques that assesses the cyber security techniques and efficiency, the focus areas include specific areas such as legal, technical, and organizational. The model uses a self-assessment questionnaire that covers a number of cyber security questions. The questions are divided into three main sections: legal, technical, and organizational. The legal section covers questions such as cyber security laws and regulations in place, the technical section covers questions on network, and data security and the business continuity strategies. The organizational section covers issues such as cyber security governance and awareness (Kravets, 2019). Table 2 shows and summarizes key

indicators and factors used in the NCSI framework when assessing the cybersecurity maturity of a country.

TABLE 2: Key Indicators and Factors Considered in the Framework (Source NCSI)

VARIABLES	ATTRIBUTES/INDICATORS
Legislation	– Legal acts – Regulations – Orders
Organizations	– Existing organizations and departments.
Cooperation Formats	– Committees – Working groups
Outcomes	– Technologies, – Websites – Programmes.

Each indicator has a value indicating its relative importance in the index. The expert group assigns the values based on the following criteria:

i. A point for a legal act that regulates a specific sector.

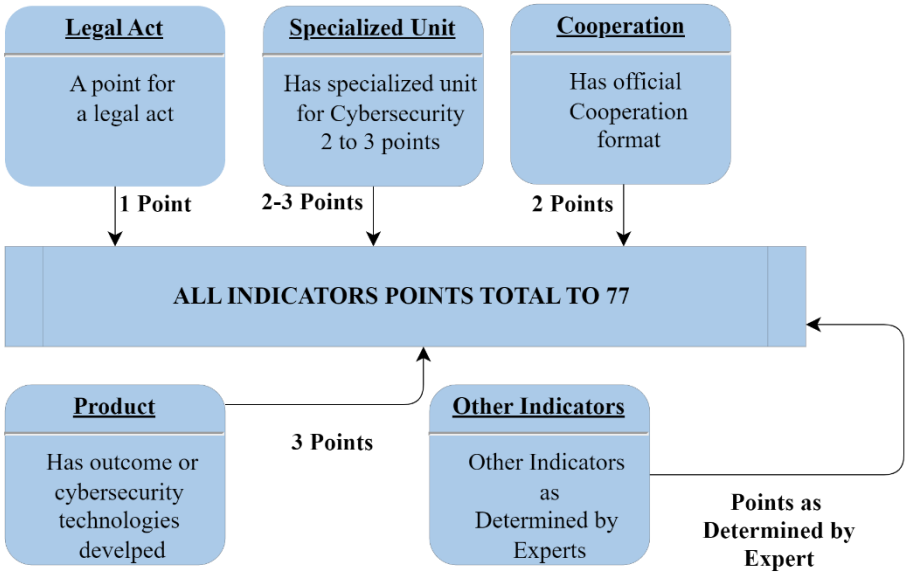
ii. 2 to 3 points for a specialized unit

iii. 2 points for an official cooperation format

iv. A point to 3 points for an outcome or a product

The country index displays the percentage of expert points awarded to the country out of a maximum possible value (currently 100% - 77 points). A graphical representation of the NCSI model is demonstrated in figure 4.

FIGURE 4 : National Cyber Security Index (Adapted from NCSI)



Limitation of National Cyber Security Index

The NCSI framework is ineffective due to a number of limitations associated with it, the limitations include: -

i. The self-assessment nature of the questionnaire may introduce bias in the results.
ii. The questionnaire may not cover all relevant cyber security issues.
iii. The results may not be directly comparable across countries due to differences in the implementation of the questionnaire.
iv. The NCSI relies on data provided by participating countries, which may not be accurate or complete. This could result in a lack of transparency and a lack of confidence in the results.

v. The NCSI is based on a set of predefined criteria, which may not fully reflect the unique cyber security challenges facing a particular country. This could lead to a lack of relevance of the results for some countries.
vi. The NCSI does not consider the specific threat landscape of a country, which could impact the overall results.
vii. The NCSI does not consider the economic impact of cyber security measures on a country. This could lead to an underestimation of the true cost of cyber security for a country (Kravets, 2019).

c) The Index of Cyber Security

The framework is based on a sentimental assessment of the risk various cybersecurity threats pose to the information system. The index was developed by New York University, Tandon School of Engineering. The index is organized as follows: attack actors, cyber weapons, the effect desired by attackers, attack targets, the vulnerability of available defenses, and overall perceptions. The ICS index evaluates risk. A higher index value indicates a more excellent perception of risk (Kravets, 2019). An expert survey of information security professionals, risk and governance officers, information security officers, scientists, and security product vendors are used for evaluation. The list of respondents is not available to the public. To ensure monthly estimates are comparable, developers keep the list unchanged issues. The responses are organized into five levels which are compared to the previous month. Table 3 gives a summary of the categories of classification of output of the response as compared to previous month outcomes.

TABLE 3: Index Levels (Source ICS, 2019)

LEVEL	DESCRIPTIONS
-20%	Fallen Fast
-7.5%	Fallen
0%	Static
+7.5%	Risen
+20%	Risen Fast

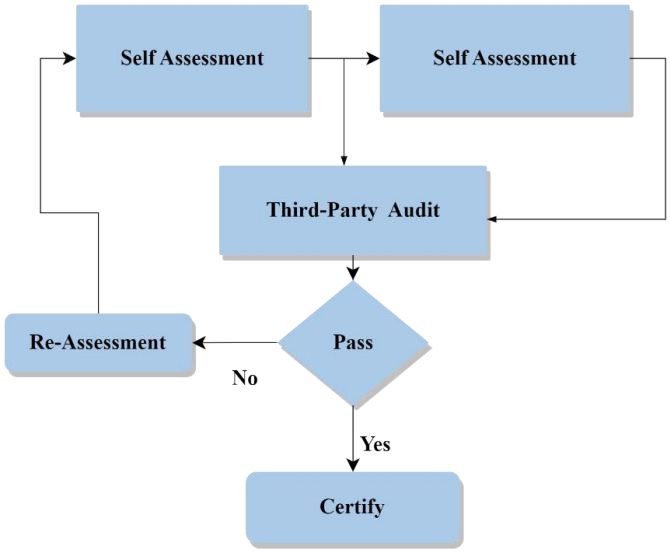
The indicators are calculated in absolute terms. Each question in the survey has a weight, and if a question has sub-questions, the weight is distributed equally among them (Kravets, 2019). Only respondents receive comprehensive feedback and comparative evaluation for each question, while the overall score level is published on the site. The optimum value tied for each question is added and divided by the total number of questions to obtain a unified evaluation from the interviewee. The ICS is determined by multiplying the preceding month's score by the total monthly estimate's exponent. There is no data verification done for ICS (Kravets, 2019).

d) Cybersecurity Maturity Model Certification

This is a model used to assess the compliance to a variety of standards published by the NIST. It consists of a combination of self-evaluations, third-party assessments, and audits. Organizations must provide documentation and evidence of compliance with the CMMC framework's security controls and practices. Self-assessment, first, organizations must assess their current cybersecurity practices and controls. They must then submit their findings to a third-party assessor. Third-Party assessment, in which organizations appoint a third-party assessor to evaluate their cybersecurity

practices and controls. The assessor will review the organization's self-assessment report as well as any additional documentation provided. The final stage is audit, in which organizations that pass the third-party assessment will be audited. A third-party auditor conducts the audit, which is intended to verify the accuracy of the organization's self-assessment and the third-party assessment. The final output is certification; organizations that pass the audit will be certified at the appropriate level of maturity. This certification is valid for three years before the organization must re-certify. Figure 5 represent a graphical demonstration of cybersecurity maturity model certification.

FIGURE 5 : Cybersecurity Maturity Model Certification (Adapted from CMMC,2020)



Limitation of the Frameworks.

The existing frameworks have not accurately and efficiently assessed, analyzed and determined the cybersecurity level in the systems due to a number of shortcomings, which include: -

i. Time-consuming and costly, as it involves a significant amount of documentation and evidence, also, the certification is only accepted by the US Department of Defense, and it does not have any legal standing, Buresh (2022) discussed the proposed Cybersecurity Maturity Model Certification rules, which will improve cyber security risk management because the proposed changes would see companies adopt a cyber risk management framework to secure the company from cyber-attacks.

ii. Subjectivity, the framework is based on subjective assessments of an organization's cybersecurity posture, which can be influenced by personal biases or perceptions. This can make it difficult to compare results across organizations or assess the framework's reliability or validity.

iii. Limited scope, while the framework focuses on best practices and principles for improving cybersecurity in the country, it may not cover all aspects of cybersecurity or be applicable to all types of systems, such as SMEs. It may also be unable to deal with emerging threats or technologies.

iv. Resource-intensive, frameworks such as the Index of cybersecurity may necessitate a significant investment of time and resources to implement, particularly for organizations at lower levels of maturity. This may limit its applicability to certain organizations and countries.

v. Lack of standards, the frameworks take different approaches to data collection and respondent selection, they lack formal standards or guidelines for implementation or use, as well as expert guidance, making it difficult to compare results across organizations or ensure consistency in the evaluation process.

vi. Lack of external validation, the framework is self-assessed, it is not validated by third parties. This can make verifying the accuracy or reliability difficult.

vii. Limited guidance, while the framework provides a general framework for assessing cybersecurity maturity, it may not provide enough guidance for implementing specific cybersecurity practices or controls, as well as grading, as a result, organizations may find it difficult to use the framework to develop a concrete plan for improving their cybersecurity posture.

viii. Limited flexibility, the framework is based on a set of predetermined levels of maturity, which may not be applicable to all systems like e-Commerce platform or all aspects of cybersecurity. This can limit the flexibility of the framework and make it difficult to adapt to the specific needs of an organization.

2.2.2 Cybersecurity Models and Standards

Cybersecurity refers to the state of being protected from cyber-attacks (P.S, 2018). The theoretical framework section of this cybersecurity assessment model is based on the concept of cybersecurity risk assessment and management in information systems such as e-Commerce platforms. The assessment process is guided by the International Organization for Standardization (ISO) 31000:2018, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (Hijji & Alam, 2022)

a) Cyber Security Canvas Model

The Cybersecurity Canvas is a model for visualizing the organization's cybersecurity program, by highlighting major items of the information technology environment. The model has four major sections, the people, process, technology, and data (KPMG, 2018). The sections include a set of key items that are essential to an effective cybersecurity risks analysis and management. The people factor considers the human elements of cybersecurity, that includes the policies, procedures, and user training that help to ensure that the user understand their roles and responsibilities in securing the organization systems. The process factor of the model, focuses on the processes and procedures that are used to manage cybersecurity risks. The technology section deals with the technology systems and techniques that that are used to secure the organization's systems, that include the firewalls, and intrusion detection systems. The data sections deal with the database that the organization process.

The Cybersecurity Canvas represents the systems in the company in graphical notation so as to gain a deeper analysis of the vulnerabilities in the system and analyse the impact and fixed the vulnerabilities before they are exploited. The model is used by the companies to evaluate and improve the cybersecurity implementation. The model is divided into four main areas: assets, threats, vulnerabilities, and countermeasures. The model follows a step-by-step process in mapping the systems assets: -

i. Assets, the first step in the Cybersecurity Canvas framework is to identify and prioritize an organization's critical assets, such as data, systems, and networks. This includes both physical and digital assets.

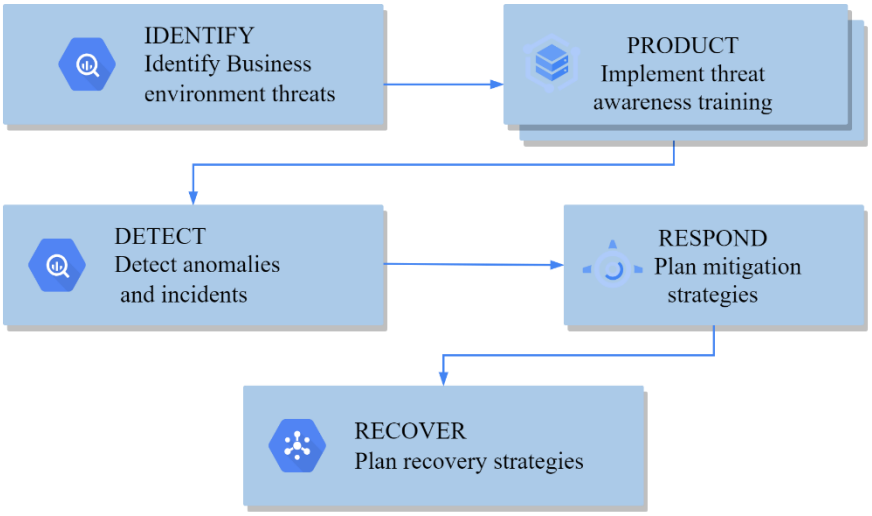
ii. Threats, once the assets have been identified, the next step is to understand the potential threats that could compromise them. This includes both internal and external threats, such as hackers, malware, and natural disasters.

iii. Vulnerabilities, the next step is to identify the vulnerabilities that could be exploited by the identified threats. This includes both technical and non-technical vulnerabilities, such as weak passwords and lack of employee training.

iv. Countermeasures, the final step is to implement countermeasures to protect against the identified threats and vulnerabilities. This comprises both technological and non-technical measures, such as training for staff members, firewalls, and systems for intrusion detection.

The Cybersecurity Canvas model provides a holistic approach to cybersecurity management, it considers both the technical and non-technical aspects of an organization's cybersecurity. It is designed to be flexible and adaptable to the specific needs of each organization and can be used to assess and improve cybersecurity at different levels of an organization, such as at the enterprise, departmental, and individual levels. Figure 6 demonstrate the cybersecurity canvas model.

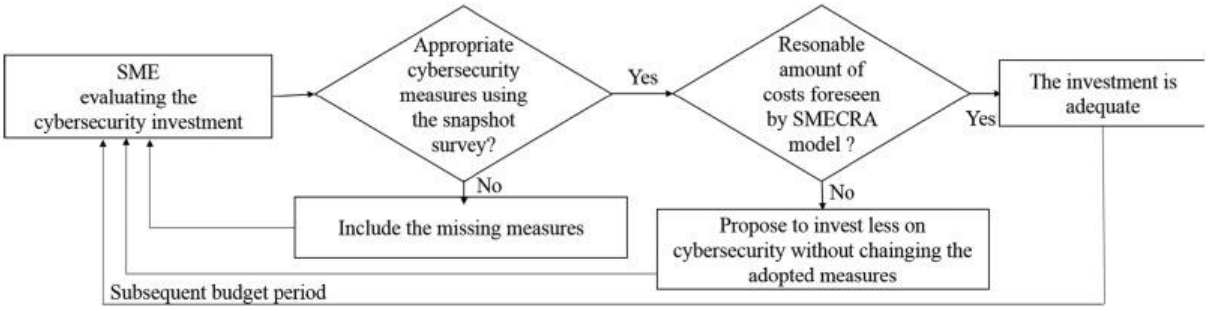
FIGURE 6 : Cybersecurity Canvas Model (Adapted from Canvas Model, 2018)



b) The SMECRA

The model is used to determine the cybersecurity implementation and status of SME cybersecurity level, it evaluate the effectiveness of cybersecurity strategies in the system (Armenia et al., 2021). The model includes a qualitative evaluation of the cybersecurity implementation and the evaluation is converted to a quantitative output. The model is used by SME as a guiding principle in determining the adoption of the third-party software, the model has best practices on the software installations, setting up security tools and password policy. The SMECRA process flow is summarized in Figure 7.

FIGURE 7: SME Cybersecurity Risk Assessment (Source: SMECRA, 2021)



The model has five steps: -

i. Security management, this involves the identification and management of the assets, identification of vulnerabilities and the risks associated with the identified assets.

ii. Evaluation, this is the second stage, it involves security assessments and penetration testing, as well as reviewing compliance to standards and regulatory requirements.

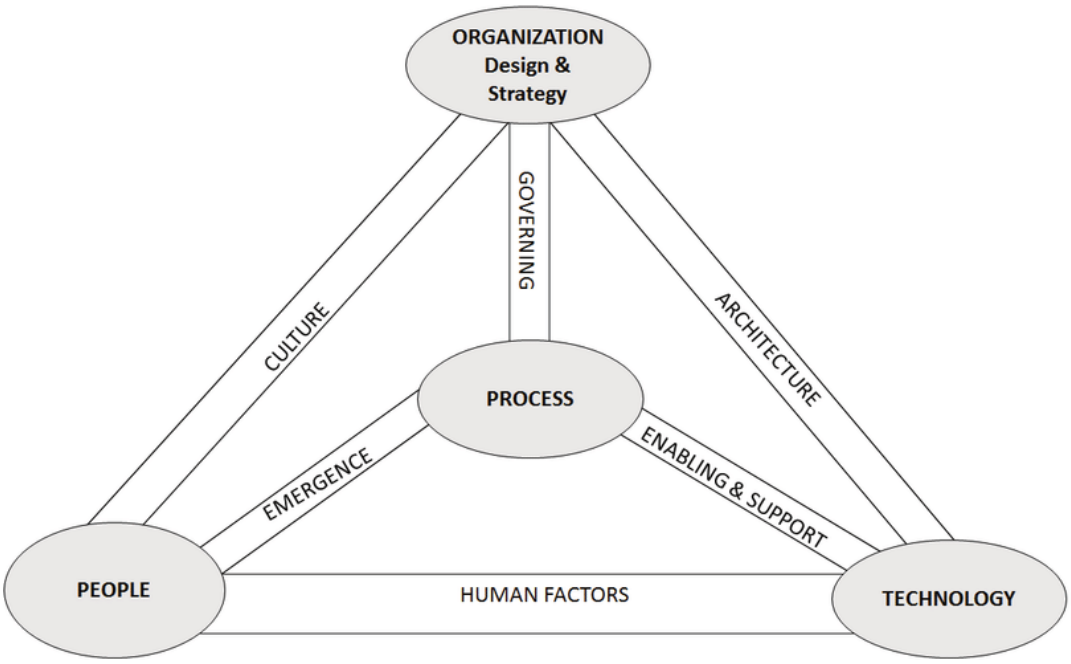
iii. Continuous risk assessment, the stage involves the continuous monitoring and assessing the cybersecurity implementation of identified assets as well the associated risks, identifying new risks and vulnerabilities. The stage has a number of activities example regular security audits and business continuity procedures.

iv. Remediation, the fourth stage involves the implementation of the countermeasures to address identified risks and vulnerabilities in the system.

v. Auditing, the final stage evaluates the effectiveness of the implemented countermeasures and cybersecurity strategies and identifying areas for improvement.

Figure 8 demonstrate the key factors considered by the SMECRA model.

FIGURE 8 : SMECRA Model (Source: SMECRA, 2021)



c) NIST Cybersecurity Framework (NCSF)

NIST Cybersecurity Framework (NCSF) was developed by National Institute of Standards and Technology (NIST), it provides a risk analysis approach as method of managing cybersecurity risks, the model provides a list of security controls and measures to be complied to by systems (NIST, 2023; Armenia et al., 2021). The framework is divided into five core functions: identify which will lead to output such as generating assets and managing it, knowing the business environment and assessing the risk and governing as well as creating the risk management strategy, the second action is protect, which create access control mechanisms, and user training and awareness, the step is followed by detect, which focused on continuous monitoring and detecting change in patterns and anomalies, the step is followed by respond, which plans for recovery and

communication and finally recover which entails recovery planning and communication(Pawar & Palivela, 2022; Sulistyowati et al., 2020).

d) ISO/IEC 27001

The standard was developed and published by the International Organization for Standardization and International Electrotechnical Commission. The standards come in a variety of versions: -

i. **ISO/IEC 27001:2013 -** This standard provides a set of requirements for an ISMS to comply in order to be considered ISO certified. Companies uses the standards to audit the compliance level, the standards enable organization to improve the systems security. ISO/IEC 27001 standard is used in organizations to manage and protect and secure information assets. Organizations use this standard to continuously review and audit their information technology environment. The standard is used to ensure the CIA triad (Sulistyowati et al., 2020) The standard is ideal for protecting personal data and commercially sensitive information. The standard covers risk assessment, incident management, and business continuity planning, among other areas (International Organization for Standardization [ISO], 2013). The steps involve getting implementation team, develop plan e.g., roles and responsibilities of the team and defining the scope of the Information security management system (ISMS) and initiate the ISMS, next step is defining the security baseline and establish the risk management process, finally implement the risk plan. Key principles of the policy are Access control policy, the information classification and handling policy. The standards guide the auditing of information systems. Organization that has a secured information system environment, or passes the audit will

be ISO certified by auditing body, the goal of the standard is to ensure the information systems assets are secured, the standard tasks managers of information systems to assess the organization's information security risks in terms of threats, vulnerabilities, and impacts and implement security controls to counter risk encountered and continuously monitor the processes to ensure that the information controls remain effective. The certification of an organization takes the following steps: -

- Stage 1: Involves checking documentations such as information system policy, Risk Treatment Plan (RTP), this stage helps the auditors familiarize themselves with the IT environment.
- Stage 2: Detailed compliance audit, testing each element against the standards, this stage needs evidence of compliance to a specific standard, if an organization passes this stage, they are certified. When an organization has been certified upon passing the audit, the certification is recognized worldwide, it confirms the compliance by the organization, this indicates that the standards have cybersecurity best practices (Culot et al., 2021)
- Ongoing Stage: this stage is a follow-up, ensuring that the organization remains compliant.

ii. **ISO/IEC 27001:2022-**This is the current revision of ISO/LEC 27001 standard. It has ten additional clauses and annex. The annex has a list of controls: -

- Organizational controls, which covers the assets, access controls, responsibilities, and management.
- People controls, which covers the remote working, security incident reporting.
- Physical controls cover physical security, securing working areas, cabling security and storage media.
- Technological controls, the data masking, data Leakage Preventions, Logging, Network Security, Web Filtering, and secure authentication.

The ISO 27001 and 27002 forms ISO/IEC 27000 family, ISO 27001 is a standard in the ISO 2700 series, it makes up the certification standards for implementation of ISMS, the organization use the ISO 27001 as a guide when implementing security practices.

e) ISO 27002

The standard provides guidance on the selection, implementation, and management of the security controls on the information systems, it supplements the ISO 27001. The standard has 14 groups of controls in clauses 5 to 18. The standard was developed for organizations who opted for some controls under ISO/IEC 27001 and wanted to implement only common security controls and develop their security management guidelines (Magnusson,2022).

The ISO 27002 is the detailed supplementary guide to standards and security controls in the 27001 frameworks.

f) COBIT 5

Control objectives for Information and Related Technologies (COBIT) is IT governance framework, it was developed by the ISACA. COBIT 5 is a framework for managing IT governance and IT management. It helps organizations align their IT strategies with their overall business goals, and provides a structured approach to managing IT risks, and improving IT performance. COBIT 5 covers five domains, including Governance and Management, IT Processes, IT Enablers, IT Resources, and Performance Measurement and Monitoring (Sulistyowati et al., 2020; ISACA, 2012). The framework was developed to counter the computer systems issues. COBIT 5 has core five principles that are used in managing the information technology environment (Horvath, 2022)

i. Principle 1: Meeting stakeholder needs, the need to address stakeholders needs because they are key in business operations and its success. The requirements of the stakeholders are well addressed in the framework.
ii. Principle 2: Covering the enterprise end to end, the framework affects the whole organization and not the IT department only. The framework assesses the entire organization risk.
iii. Principle 3: Applying a single integrated framework, it includes the employees and departments, processes and management and governance and this accurately identifies the risks and threats and how to ensure efficiency in services delivery.
iv. Principle 4: Enabling a holistic approach, provision of holistic approach in process improvement and efficiency.

v. Principle 5: Separating governance from management, aligning the governance with IT governance, removing governance part from management, and integrating the IT governance and enterprise Governance (Sulistyowati et al., 2020).

The framework is resourceful to managers of organizations in understanding IT governance and the integration of IT governance and enterprise-wide governance (Maseko & Marx, 2016).

g) Payment Card Industry Data Security Standard

Developed by the Payment Card Industry Security Standards Council, PCI DSS is a set of security standards designed to protect cardholder data and prevent credit card fraud. Its implementation is to provide a benchmark standard for securing cardholder (Seaman, 2020). Organizations that accept credit card payments must comply with these standards, which include requirements for security management, policies, procedures, network architecture, and software design (Payment Card Industry Security Standards Council, 2016). The organizations that take a proactive approach in standards compliance may be able to win the market share from security-conscious market segment (Bradley, 2007).

The standards guide in developing secure network and systems and protecting the cardholder data and ensuring there is monitoring of the vulnerability. The standards ensure strong access controls monitoring of anomalies in the systems and networks. The main goal of the standard is to manage the credit card fraud by ensuring better controls are in place for sensitive credit card customer data, and no data is exposed (Wikipedia, 2023). The major card brand had private ordering for the development of the standard to avoid the threats of legal liability (Morse & Raval, 2008). The standards have a timelines and schedule for running the test to ensure

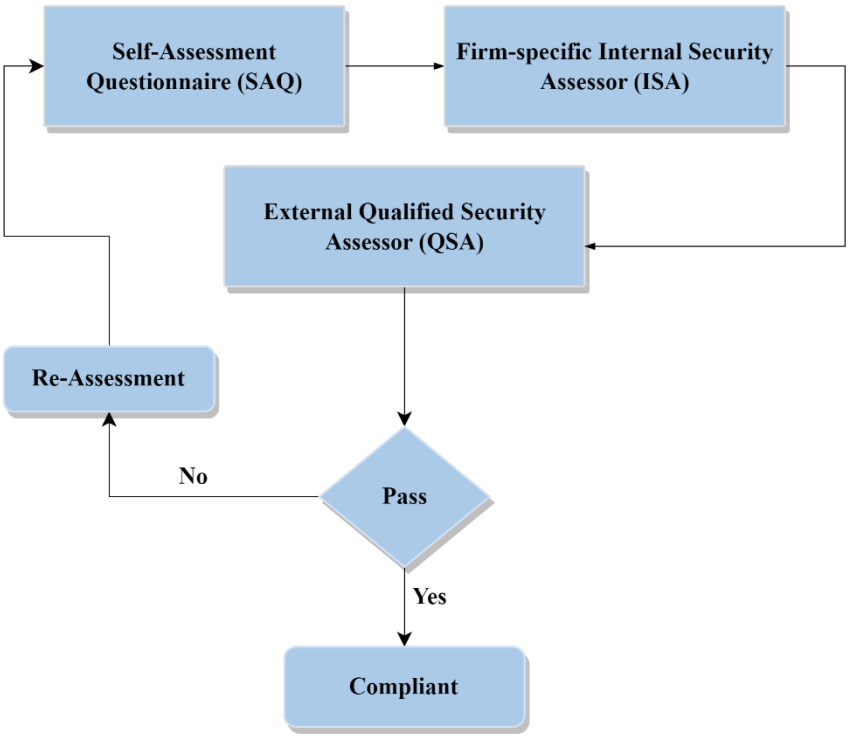
compliance, the standards compliance runs every three months and one at the end of the year. The standard assesses the payment gateway using three entities and tools, these includes: -

i. The Self-Assessment Questionnaire (SAQ), which consists of validation tools that help organizations report the results of their PCI DSS self-assessment.
ii. The Firm-specific Internal Security Assessor (ISA), who is an entity or person from the organization who can perform PCI self-assessments for their organization.
iii. The External Qualified Security Assessor (QSA), who is an entity certified to audit the compliance by merchants for Payment Card Industry Data Security Standard (PCI DSS)

The PCI standard was as result of interoperability issues experienced by major credit card controllers, the Visa, Mastercard, American Express, Discover and JCB were the major card brands each had its own security standards assessing and ascertaining that any company using their payment gateway met the standards for them to store, process and transmit the customer credit card data. The companies had different methodologies of assessing the compliance of their defined standards and that led to PCI standard for standardized approach of assessing the card standards.

Figure 9 shows the PCI DSS process flow.

FIGURE 9 : Payment Card Industry Data Security Standard (Adapted from PCI DSS)



The standard has a specific requirement that guides the compliance, these includes: -

i. The Network and Systems should always be secured.

ii. The cardholder data should be protected.

iii. The Vulnerability Management Program should be in place.

iv. Develop and implement strong access controls measures.

v. Regular Network tests and monitoring

vi. Information System Policy should be in place.

The requirements above have a subcategory for assessment, in addition to the sub requirements above, there are twelve high level requirements that remain unchanged even with versioning of the standards (Sulistyowati et al., 2020). The requirement or sub-requirements are guided by the following steps: -

i. Standard Requirement, which states and defines the requirement, details all that it entails about the requirement.
ii. Testing and assessing process, that details the process of assessing the requirement, defines the methodologies that should be followed by the assessment team to ensure that the right process is followed and that accurate results are obtained.
iii. Guidance, this justifies the need for the requirements in the compliance and the input and output of the requirements.

The twelve requirements are as follows: -

i. Install a firewall to protect cardholder data.
ii. Do not use the default credentials for systems login.
iii. Protect the cardholder data.
iv. Encrypt cardholder data on transit when done over open and public networks.
v. Protect systems against malware.
vi. Develop secured systems and applications.
vii. Restrict access to cardholder data.
viii. Identify and authenticate access to system components.
ix. Restrict the physical access to cardholder data storage location.

x. Monitor all access to network resources and cardholder data.

xi. Continuously test security systems and processes.

xii. Have an information security.

PCI Security Standards Council Published Version 1.2 of the Secure Software Standard and Program, the version focuses on software security, ensuring that the payment software is designed, developed, and maintained in a manner that secures payment transactions and data, reduces vulnerabilities, and defends against cyber-attacks by implementing security controls against web software attacks. “The PCI Secure Software Standard is designed to offer a more flexible approach to how we test the security and integrity of payment software,” said Emma Sutcliffe, SVP Standards Officer, (PCI Security Standards Council PCI Security Standards Council, 2022)

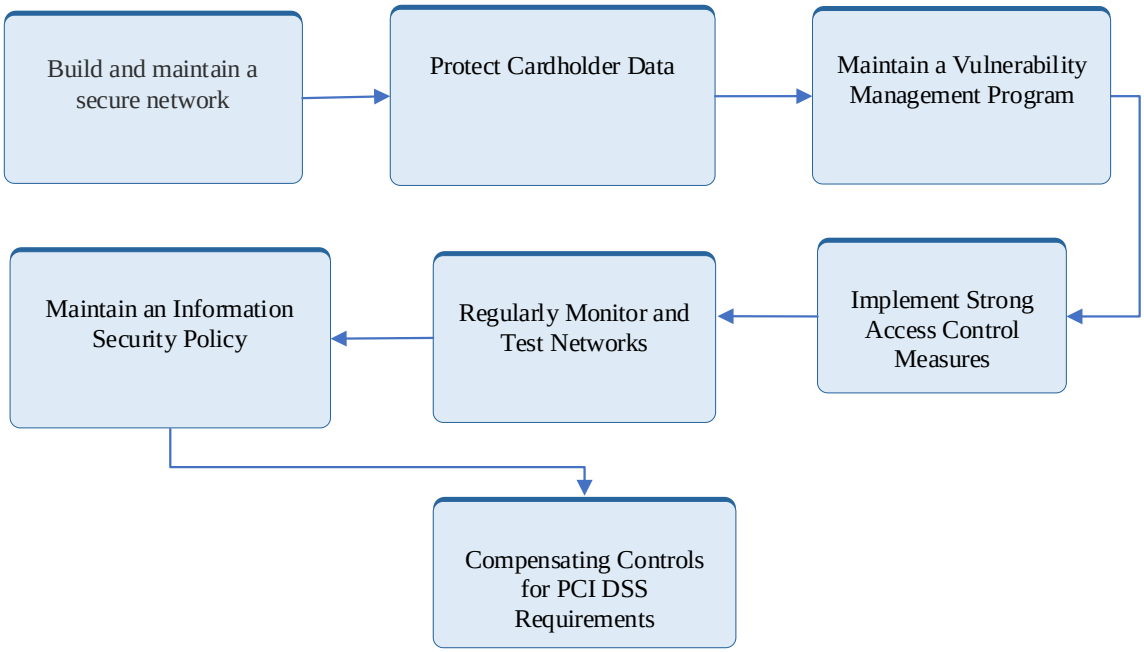
i. The version introduced four high-level requirement areas: -
ii. Documenting and monitoring the use of open-source software and third-party applications and related APIs in payment software.
iii. Controlled access to payment software web APIs and other critical assets
iv. Mitigating common web attacks
v. Protected communications between web-based payment applications.

PCI DSS compliance is a voluntary process for any organizations and is not a requirement of federal law in the United States hence not addressing the practicality, the standard can provide an additional layer of security to card holders, for the standard to achieve such security some additional cost is passed to the merchants (Morse & Raval,2008). Rees (2012) study found that

merchants limit the assessment scope and opt for third parties for costly controls as they assess their compliance.The PCI initially focused on very large merchants which had large transactions in a financial year, there was some progress on the compliance and the council shifted focus to SMEs, due to the cost of implementation of the standard the PCI council in 2015 decided to create a taskforce to guide in improving small merchant credit card data security, this pushed non-compliant SMEs to be compliant.,even with the taskforce only slightly more than ten percent of the small businesses are compliant with PCI DSS (Clapper & Richmond, 2016).

Figure 10 shows the flow of PCI software securing process.

FIGURE 10: Payment Card Industry Data Security (Source: PCI DSS, 2022)



2.3 Empirical Perspectives

a) Risk Management in Digital Lending

Innovation in Banking sectors has been driven by the need to remain competitive, with innovation comes technological risks and hence the need for strong technological risk management. Moturi & Ogoti (2020) used RiskIT model from ISACA in assessing the technological risks of mobile lending technologies in regulated and unregulated digital lending firms, the RiskIT model helps organization to manage their technological risks, the model adopted three variable in assessing the Risk management, that is: the governance, evaluations and the response and relationship between the variables, the weakness in technological risks which resulted in exposure to technological risk prompted the researcher to investigate the technological risk management among the digital lending platforms in Kenya. The findings found that the regulated digital credit providers had a strong risk management for their digital lending platforms, the unregulated organizations had weak risk management (Moturi & Ogoti, 2020). The Moturi & Ogoti (2020) study used data as provided by the population studied.

b) ISO/IEC 27001 Information Security Management Standard to SMEs

Ramadhan & Rose (2022) studied the role of ISO/UIEC 27001 as a cybersecurity framework in SMEs, and its implementation, and suggested the most relevant framework for SMEs to manage their cybersecurity as well as create awareness on SMEs on best practice of adapting the framework. Most ISMS have been exposed to vulnerabilities and the CIA triad is not the case in most information systems. Cybersecurity controls should be standardized in all systems (Wong et al., 2022). The Ramadhan & Rose (2022) study detailed that ISO 27001 supports the Wong et al.,

(2022) need for standardization of cyber security controls, and that it helps the SMEs to ensure that account management, security of data and application access controls are in place and effective. Companies should have security measures in place for their ISMS (Nagata et al., 2022). The researcher found that most SMEs have a challenge when implementing ISO 27001 since it was developed to be implemented by professionals and most SMEs do not have in-house cybersecurity experts. The study findings included mistrust in the standards, also the privacy factor made the SMEs to resist adoption of the standards (Ramadhan & Rose, 2022)

c) Framework for Risk Management in SMEs

Mthiyane et al. (2022) study focused on determining how SMEs handle risk management and proposed a framework to enable SMEs to adopt the enterprise risk management (ERM). The study focused on accounting information. The study determined the importance of information governance and pillars of risk management in SMEs. Mthiyane et al. (2022) agrees with Ferreira De Araújo Lima et al. (2020) arguments that the ERM has not been sufficiently developed for use in SMEs, this can be attributed to the poor information governance and the lack of guidelines on factors promoting the ERM among the SMEs. The research findings were that the SMEs have limited resources to implement the ERM, and called for simplified ERM, and a comprehensive implementation guide developed.

2.4 Cybersecurity Challenges Faced by SMEs in Kenya

SMEs in Kenya have increasingly adopted e-Commerce platforms to reach new customers and expand their businesses operations in Kenya and globally. According to the Kenya National Bureau of Statistics (KNBS), Kenya has 7.41 million SMEs, there adoption of e-Commerce platforms by

SMEs in Kenya has brought about several cybersecurity challenges. These challenges can range from data breaches, payment fraud, and cybercrime, to social engineering attacks, and unsecured networks (Muhati, 2018). According to the Communications Authority of Kenya (2021) cybersecurity report, at least 38 million SMEs reported cases of cyber-attacks between January and April 2021. Malicious software, also known as malware, was responsible for 51% of these incidents. A 47% increase in internet attacks in 2022 was recorded among SMEs in Kenya, (Kaspersky, 2022).

a) Data Breach

Data breach is one of the challenges faced by the SMEs in Kenya, data breach is a security incident in which sensitive, confidential, or protected data is accessed and used or disclosed and transferred without authorization of access control officers in the company (Cheng et al., 2017b). Data breaches can occur due to various reasons, such as hacking, malware infections, insider threats, weak passwords, unpatched vulnerabilities, SQL injection and cross-site scripting (XSS) attacks, and social engineering attacks.

In research by Mwangi et al. (2017) 76.2% of survey participants had experienced data breaches in the previous 12 months of study, with backup malfunction being one of the breaches. According to Namunwa (2021), 58% of SMEs are not prepared to counter malware attacks. Recurring financial fraud can plainly show that the firewall was ineffective at stopping hacking, and that there was a data breach, and no access restrictions or role-based controls in place. A data breach can severely compromise user data such as names, addresses, social security numbers, and

credit card information, as well as confidential business information and intellectual property (Cheng et al., 2017).

b) Unauthorized Access

Unauthorized access to sensitive information refers to the process of accessing data or systems without proper authorization or permission (Shi et al., 2020). This can happen when cybercriminals gain access to a network or system through hacking, social engineering, or insider threats. Unauthorized access can also occur when an individual or group within an organization accesses data or systems that they are unauthorized to access, such as accessing confidential information without a valid reason. SMEs in Kenya has a challenge of unauthorized access, Murigi (2017) study discovered that most businesses had experienced unauthorized access in the previous year of study.

c) Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) attacks is one of the main challenges for SMEs in Kenya. These types of attacks involve multiple computers and networked devices flooding a target network or website, example an e-Commerce platform with a large volume of traffic, causing it to become unavailable to users. This can result in significant business disruption. SMEs in Kenya are vulnerable to DDoS attacks due to limited resources and budget for cybersecurity measures, widespread use of the internet and digital technologies in their operations, and a lack of technical expertise to address cybersecurity incidents. Ngugi (2016) study discovered that the main challenge for SMEs in managing e-Commerce security threats was financial constraints. DDoS

attacks can cause slow or delayed service response or complete system lockout (Bhatia et al., 2018).

d) Lack of Resources to Address Cybersecurity

Several SMEs in Kenya do not have the financial resources or technical expertise to invest in cybersecurity measures. This leaves them vulnerable to cyber-attacks, which can result in financial losses, and loss of sensitive information. SMEs do not have the resources to hire an internal cybersecurity professional and only devote a small budget for cybersecurity (Mwangi, 2021; Satyanarayana et al., 2022). Table 4 provides an overview of the existing knowledge gaps pertaining to models, frameworks, standards, and empirical research.

TABLE 4: Knowledge Gaps

RESEARCHER(S) AUTHOR(S)	STUDY FOCUS	FINDING(S)	KNOWLEDGE GAP & LIMITATION	STRATEGY
Ramadhan & Rose (2022)	ISO/IEC 27001 FOR SMEs	Limited resource hinders implementation. Limited to Cybersecurity Experts to implement. SMEs mistrust the standard. Privacy of SMEs hindered adoption.	Failed to propose an alternative framework for SMEs.	Propose a cost effective and comprehensive model tailored to Unique needs of e-Commerce Platforms
Payment Card Industry Data Security Standard (PCI DSS)	Payment Card standards	Provision of standards to credit card data processing. Data Privacy	Voluntary Reliance on data from Organizations	The model will adopt a simple implementation, well guided objective methods

RESEARCHER(S) AUTHOR(S)	STUDY FOCUS	FINDING(S)	KNOWLEDGE GAP & LIMITATION	STRATEGY
			No clear Validations Methods Complex methodology Limited to Payment Cards	
ISO/IEC 27001	Global Cybersecurity Standards	Provision of global standards for Cybersecurity practices	Subjective, dependent on data provided by the organizations. All-in one fit Expensive.	Validated tools. Simple implementations
COBIT 5	IT & Entreprise Governance	Provisions of guidelines on IT Governance and Enterprise Governance and need for separation of Governance and management	Complexity, it brings in the IT and Enterprise Governance. All-in one fit., do not address the unique factors of specific systems. Resource Intensive, the variables and factors considered needs resources to integrate and assess them	The proposed model will address the core of cybersecurity challenges and not just focusing on the governance.
Cybersecurity Maturity Model Certification	Certification of Compliance	Provision of standardized cybersecurity evaluation methodology. The incident Response Methodology Best Cybersecurity practices.	Complex for SMEs High Cost, the stages taken has cost related attached. Time Consuming due to steps taken. Resource Intensive needs	Cost and time effective model. Capture unique needs for SMEs.

RESEARCHER(S) AUTHOR(S)	STUDY FOCUS	FINDING(S)	KNOWLEDGE GAP & LIMITATION	STRATEGY
			personnel and time. Lacks Flexibility do not consider Unique needs of different systems.	
The Global Cybersecurity Index	Cybersecurity Index of Countries	Cybersecurity awareness Cybersecurity Best Practices Evaluation and Guidance	Subjectivity, based on self-assessment. Limited scope, no key cybersecurity factors considered in evaluation. Lack of uniformity. Limited data availability relies on data provided by countries. Lack of update, updated once in a year, this do not reflect changing posture of cybersecurity	The proposed model will be based on validated data,
Cyber Security Canvas Model	Risk-based Cybersecurity Assessment	Holistic cybersecurity evaluation Risk-based approach, identify assets and risk associated with them. Collaboration in cybersecurity assessment	Resource Intensive. Complexity needs experts. Lack of standardization. Subjectivity, due to dependence on self-assessment	The proposed model will adopt objective assessment
SMECRA (Security Maturity Evaluation and	Risk-based Cybersecurity Evaluation	Cybersecurity Maturity evaluation	Resource Intensive, time	Resource efficient model

RESEARCHER(S) AUTHOR(S)	STUDY FOCUS	FINDING(S)	KNOWLEDGE GAP & LIMITATION	STRATEGY
Continuous Risk Assessment)		Risk-based approach Continuous improvement Compliance to standards. Cybersecurity Collaboration	and expert needed. Complexity, need technical expertise. Lack of standardization on implementation. Subjectivity, dependence on self-assessment. Limited scope, does not consider key cybersecurity factors.	Simple implementation
NIST Cybersecurity Framework (NCSF	Cybersecurity Standards	Risk management. Industry standard Integration with existing standards. Collaboration in Cybersecurity. Compliance enforces standards	Complexity and Intensive resource requirements, need time, resources, and expertise. Limited prescriptiveness, it provides guidance and not standards.	Unique needs of e-Commerce will be addressed in the model
Mthiyane et al. (2022)	SMEs Risk Management ERM	Limited resources to implement ERM by SMEs SMEs challenged by complex ERM implementation. The need for comprehensive guide on implementation of ERM	Failed to propose an alternative simple and resource efficient framework	Will consider resource and implementation requirements in the proposed model

RESEARCHER(S) AUTHOR(S)	STUDY FOCUS	FINDING(S)	KNOWLEDGE GAP & LIMITATION	STRATEGY
Moturi & Ogoti (2020)	RiskIT framework for Digital Lending	Regulated digital lending firms are compliant while unregulated are not compliant.	Focus on compliance and not security of digital lending firms	The proposed model will focus on security and not compliance, state of security of the e-Commerce platform.

2.5 Conceptual Framework

This cybersecurity assessment model was designed specifically for e-Commerce platforms in this research but do not limit the use case to e-Commerce platforms, with a focus on six key areas: access controls, software security, data security , authentication and authorization, and network security, as per Cheng et al.(2017b), research, e-Commerce cybersecurity threats included SQL Injection, ports and services, denial of service, and social engineering, these factored in the objective number (ii), the key cybersecurity factors that should be considered in an assessment model and subsequently development of a comprehensive model to assess cybersecurity implementation in B2C e-Commerce and in doing that objective number (iii) was realized. The aim of the model was to develop a comprehensive and unbiased method for evaluating the cybersecurity implementation and vulnerabilities of e-Commerce platforms and to offer practical recommendations for enhancing their security and compliance to secure the protection of user data and operations. The aim was to establish an objective cybersecurity evaluation so that SMEs in Kenya can evaluate the platform's security posture and secure their customer data and corporate assets from online threats.

2.6 Cybersecurity Assessment Variables & Attributes

2.6.1 Access Control

This variable assessed vulnerabilities that allows unauthorized access, example OpenSSH Security Bypass Vulnerability, the brute force attacks, and session hijacking, assessing the e-Commerce session management controls, this helped identify vulnerabilities in the platform's session controls. The variable also assessed the role and privilege escalation vulnerabilities. The variable had a total

of 20 points, each attribute took 5 points and reduced with any vulnerability identified. The Greenbone Vulnerability Management (GVM) and Metasploit was used to collect data on Access Control and the results were exported to XML and SQL. The variable had the following attributes: Role Escalation, Privileges Escalation, Access Control Bypass, and Brute Force Attack

2.6.2 Network Security

This variable assessed the hosting environment, determining whether network mapping was possible by attempting to map out the platform's network infrastructure, including hosts, servers, and devices, to identify potential vulnerabilities and attack vectors and determining open ports and services that can be exploited. Assessed the infrastructure of e-Commerce by gathering information and determining exploitability. Determined if there was remote access enabled. Evaluated the Denial of Service (DoS) attack by attempting to disrupt the availability of the platform's network infrastructure, this was determining by overwhelming the e-Commerce platform with excessive traffic or alternatively it was determined by identifying vulnerabilities associated with DoS. Cloud security testing was also done, if the e-Commerce platform was hosted on cloud infrastructure, security of the cloud environment was evaluated, and identified any misconfigurations or vulnerabilities. The variable had 5 attributes (Network Mapping, Port and Services, DoS Attacks, Remote Access, and Cloud Security) each having initial 3 points and totaling to 15 if the evaluated indicator did not have any vulnerability that could be exploited.

2.6.3 Data Security.

This variable evaluated the SQL injection capability, this was achieved through an attempt to inject malicious SQL code into the platform's database to gain unauthorized access to sensitive data or disrupt the availability of the database, the variable had a binary evaluation. The second attribute was Cross-site scripting (XSS) and file inclusion vulnerabilities, evaluating an attempt to inject malicious code into the platform's web pages. The variable also had data leakage attribute, information gathering to identify any sensitive data that was being transmitted or stored on the platform in an unsecured manner. Data encryption testing was evaluated to identify any unencrypted sensitive data that is being transmitted or stored on the platform. Data retention testing was evaluating any weaknesses in the platform's data retention policies and procedures, including testing if deleted data could be recovered and testing if all required data was kept for regulatory compliance. SQL injection tests was performed using SQL map, which identified issues and vulnerabilities. SpiderFoot and Intrigue was used at the start of data collection and information gathering to gather as much information as possible about the target, including names, email addresses, domain names, IP addresses hostname, network subnet, email address or person's name, and other exposed details about the target. BeEF-The Browser Exploitation was used to evaluate e-Commerce platform from a perspective of a web browser to determine its security. The variable had 5 attributes totaling to 35 points, SQL Injection 15 points, Cross-site Scripting 5 points, Data Leakage 5 points, Data Retention and Encryption 5 points, and File Inclusion 5 points.

2.6.4 Software Security

The assessment covered the Web Application Firewall (WAF) testing, evaluating the effectiveness of the platform's web application firewall in protecting against web-based attacks. Evaluation of the third-party plugins and integrations testing, focused was given to the security of any third-party plugins or integrations that were being used by the platform to identify any vulnerabilities or misconfigurations. The third attribute was the Payment gateway testing, evaluating the security of the platform's payment gateway to ensure that it could protect sensitive payment information and that it followed relevant regulations and industry standards. The variable covered 3 attributes (Web Application Firewall, Third Party Apps, and Payment Gateway), total points 15, each attribute had 5 points. The Greenbone Vulnerability Management (GVM) framework was be used to collect data on software parameters.

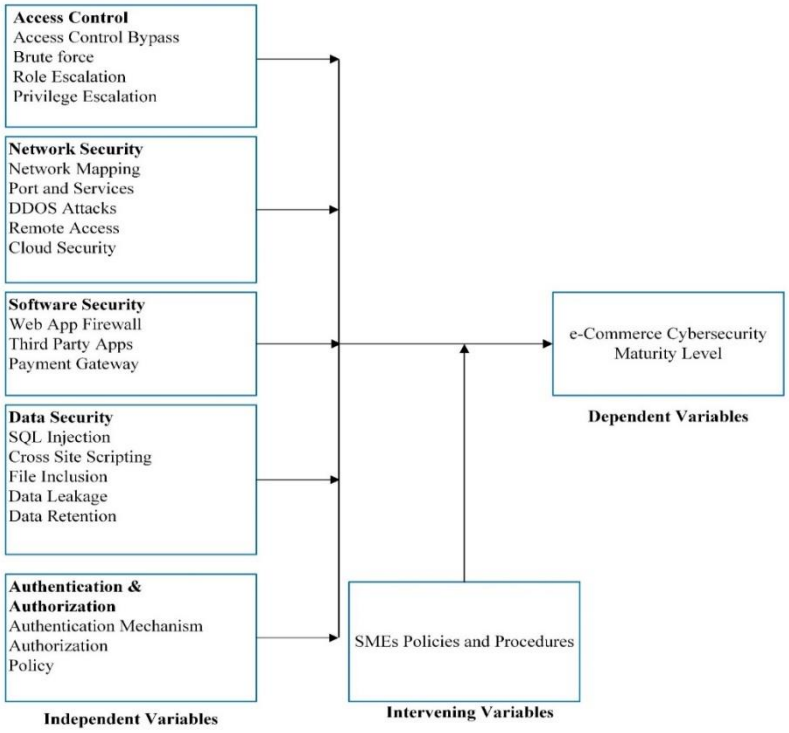
2.6.5 Authentication and Authorization

This variable evaluated platform's authentication mechanisms, such as username and password, multi-factor authentication, or biometric authentication to identify any weaknesses or vulnerabilities. Authorization testing, testing the platform's authorization mechanisms, such as role-based access control, to ensure that users could only access the resources and data that they were authorized to access, example store manager role, administrator role and customer. Password policy evaluation was another attribute in this variable, testing the platform's password policy to ensure that it enforced strong and complex password. The two-factor authentication evaluation determined the platform's two-factor authentication mechanisms to ensure that they prevented unauthorized access. The attribute had 15 points, attributes included Authentication Mechanisms

which, 5 points, Authorization mechanism, 5 points and Password policy, 5 points. This category was evaluated using practical test cases.

Figure 11 shows a graphical representation of the conceptual framework.

FIGURE 11 : Conceptual Framework



2.7 Operationalisation of the Variables

TABLE 5: Operationalization of the Variables

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
Access Control	– Privilege Escalations, – Role Escalations – Access Control Bypass, – Brute Force Attacks.	For any CWE and outputs corresponding to an indicator calculate points by using the metric: - $= 3 - \frac{Severity(IndicatorPointsxQoD)}{10x100}$ – The indicator having more than one occurrence of vulnerability and	**±20**

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
	Tools – gvm – dnsenum – Start the GVM. – Platform, IP – Hydra	total points exceeding the maximum point will be assumed to have deducted the total points. – CWE-284, CWE-285, CWE-287, CWE-288, CWE-289, CWE-290, CWE-292 – CWE-293, CWE-294, CWE-298CWE-300E – Man-in-the-Middle Vulnerability. – Bookmark Security Bypass Vulnerability – Privilege Escalations Vulnerability – Unauthorized Access Vulnerability – Remote Code Execution Vulnerability – Brute force-Account Lockout – Access Control Bypass-HttpOnly Flag – Role Escalations Access-Anti-CSRF tokens – Privilege Escalations-Cross Origin Resource Sharing (CORS),	
Network Security	– Network Mapping, – Port and Services, – DoS Attacks, – Remote Access – Cloud Security Tools – GVM – Dnsrecon	For any CWE and outputs corresponding to an indicator (– Network Mapping (Pathname to a Restricted Directory, Directory Listing), – Port and Services (SSH Weak Encryptions), – Cloud Security (End of Life Detections, Missing Encryption of Sensitive Data.)	**±15**

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
	– Whatweb – sslscan – Dmitry – amap	– Remote Access (Weak Encryptions, Command Vulnerability, Use of a Broken or Risky Cryptographic Algorithm, Improperly Restricting URL Access) Calculate points by using the formula. $= 3 - \frac{Severity(IndicatorPointsxQoD)}{10x100}$ The indicator having more than one occurrence of vulnerability and total points exceeding the maximum point will be assumed to have deducted the total points. **Additional Notes** – Assess SSL (sslscan) – Assess Ports and Services(amap) – CWE-200, CWE-295, CWE-296, CWE-307, CWE-311, CWE-312, CWE-327, CWE-297 – SSH Weak Encryptions – Directory Listing – Command Vulnerability – Weak Encryptions – End of Life Detections – HTTP STRICT Transport Security HSTS missing. – TCP timestamps – SSL/TLS hostname discovery from certificates	

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
		– Error Reporting – Cross Site Request Forgery	
Data Security	– SQL Injection – Cross-Site Scripting – File Inclusion – Data Leakage – Data Retention Tools – JSQL – SQLNINJA – SQL Map – Dir search – Maryam – wfuzz – The harvester	For any CWE and outputs corresponding to an indicator (Cross-Site Scripting, Data Leakage) calculate points by using the metric. $= 4 - \frac{Severity(IndicatorPointsxQoD)}{10x100}$ The indicator having more than one occurrence of vulnerability and total points exceeding the maximum point will be assumed to have deducted the total points. – SQL Injection will have a binary evaluation, where there is SQL Injection capability deduct 15 points otherwise allocate 15 points. – Data Retentions Policy Will be a binary evaluation, presence will +5 while absence will deduct 5 points. – CWE-89 and CWE-912, CWE-913, CWE-919: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'): validate user input, which can lead to the injection of malicious SQL code into a web application. – CWE-564: SQL Injection – CWE-891: SQL Injection in a Web Application Framework: – CWE-312: Cleartext Storage of Sensitive Information – vulnerable URLS	**±35**

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
		– List of Enumerated user, password hashes, tables, databases, columns. – User Detections – XSS Attack – SQL Injection Vulnerability – Input Sanitation, Validation Vulnerability Assess data retention mechanisms, Binary (1,0, implemented or not implemented, if 1, access its functionality, data retained after deletion request?) Data Leakage Assess enumeration of user, password hashes, tables, databases, columns	
Software Security	– Web Application Firewall – Third Party Apps – Payment Gateway Tools- – CMSeeK – GVM – wafw00f	Web Application Firewall will have a binary evaluation, where there is no WAF deduct 5 points otherwise allocate 5 points. Third Party Apps, for each outdated Version Deduct 1 point up to 5 points otherwise allocated where there is stable version installed. Payment Gateway Check – The payment gateway installed meets ISO standards, fraud prevention measures. – PCI compliance – accessibility of support – Version C**WE & Vulnerabilities**	**±15**

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
		– CWE-119: Memory Buffer: – CWE-120: Buffer Copy without Checking Size of Input (– CWE-121: Stack-based Buffer Overflow: – CWE-122: Heap-based Buffer Overflow: – CWE-191: Integer Underflow – CWE-194: Integer Overflow or Wraparound: – CWE-197 – CWE-200: Information Exposure: – CWE-295: Improper Certificate Validation: CWE-312: Cleartext Storage of Sensitive Information – Multiple Security Vulnerabilities – Binary evaluation of Web Firewall, – Evaluate third party apps, custom coded apps or standardized apps for payment gateway and third-party applications. – Check Versions of Apps – Plugins and Third-Party Apps – Backup files Finder – Core CMS Vulnerability. – Directory Listing – Configuration files leaks, Themes	
Authentication and Authorization	– Authentications Mechanisms. – Authorization Checking	For any CWE and outputs corresponding to an indicator (Authorization Mechanisms) calculate points by using the metric The indicator having more than one	**±15**

VARIABLES /FACTORS	ATTRIBUTES	ASSESSMENT METRICS	MAX SCORE
	– Methods of Authentications, passwords, biometrics, or combination of 2FA. – Password Policy	occurrence of vulnerability and total points exceeding the maximum point will be assumed to have deducted the total points. Authentication Mechanisms will be a binary evaluation, reliance on one authentication mechanisms will evaluate to zero points while two or more will yield 5 points. The policy items (password policy, Passwordless login, cleartext login, weak password, login attempts) will each have **±5** – CWE-287, CWE-288, CWE-289, CWE-290: CWE-291, CWE-308: CWE-306, CWE-307 – Password Policy- Reliance on a Single Factor Authentication – Weak Passwords – Unlimited Login Attempts – Passwordless Login – Unencrypted Cleartext Login	
Totals			**±100**

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The research methodology defines and states the how of the research, it documents how the research was carried out. It details the principles for organizing, planning, designing, and conducting research, that guided the study (Mohajan, 2017). The chapter details the mixed-methods research design, the populations, the sampling methods, and the data collection methods and analysis that were adopted for the research. The chapter detail the research design that the study used and the how of data collection, analysis, and discussion.

3.2 Research Design

The study utilized the experimental design. This research design was used to objectively assess and evaluate how effective various cybersecurity implementation were in the e-Commerce operated by the SMEs in Kenya (Sassower, 2017). The design allowed recording of observations of the test cases which was achieved by using a specialized cybersecurity tool, the observations recording involved both qualitative and quantitative, the test cases were guided by the observation checklist (Cash et al., 2016). The research design enabled the researcher to record the output of test cases under different condition and validate the findings obtained under different conditions.

The design facilitated the researcher to assess the CWE and the vulnerabilities in the e-Commerce website. The design also made it possible for the researchers to evaluate different combinations variables and evaluate the individual and combined impacts on e-Commerce security. The vulnerability detecting tools and the penetration testing frameworks and solutions like Greenbone Vulnerability Management, Metasploit, and Maltego provided means for the

researcher to collect quantitative and qualitative data from the platforms. To offer objective, measurable statistics on the security of the system or network, quantitative data collection methods such as vulnerability scanning, and penetration testing were used. The information gathered was critical in identifying patterns and trends, as well as evaluating potential risks and weaknesses. To examine the quantitative data and uncover patterns and trends, quantitative data analysis approaches such as statistical analysis were utilized. To find patterns and themes in the qualitative data, qualitative data analysis approaches such as content analysis were applied. In the piloting assessment process, an experimental design was implemented on SMEs; it was used to analyze their cybersecurity strategy, finding strengths and shortcomings while evaluating and fine tuning the research data collections tools. The participant observation, test cases, and empirical tests all were useful in determining vulnerability, test vulnerability, and the impact on SMEs platforms. The experimental design was also used to test the model's validity and reliability by changing variables that determined the output of the data collection instruments.

3.3 Target Population.

According to Ali et al. (2022), target population is defined as records or events, people that composed the researchers' point of getting information. The target population was the source of information required. The research targeted five categories of B2C e-Commerce, Cosmetics, Electronics, Fashion, General Stored, Booking, and Grocery run by SMEs, the target population included 113 SMEs who operates e-Commerce in Kenya. The target population highlighted five strata of focus, this included Cosmetics, Electronics, Fashion, General Stores, Booking, and Grocery. Table 6 summarizes the five strata that were selected to represent the target population.

TABLE 6: Target Population (Source: Research)

CATEGORY	NO. OF SMES	PERCENTAGE (%)
Cosmetics	40	35
Electronics	37	33
Fashion	13	12
General Stores	11	10
Booking	7	6
Grocery	5	4
Total	**113**	**100**

3.4 Study Population and Sample Size

The research sample is the entities whose data were collected. They are the members of the population; each category of e-Commerce was selected to represent the entire population and avoid biases, since the e-Commerce is based on same architecture, the strata used did not represent the unique operations of the SMEs rather than the e-Commerce architecture, hence the different number of sample size for each stratum. These sources of data enabled the researcher to understand the status of cybersecurity maturity, challenges and how cybersecurity assessment was being done making objective I of the research achieved. A good sample design will result in minimal sampling errors; the researcher determined the entities to collect data from. The research employed a combination of census and purposive sampling methods. Census sampling was utilized to include all eligible e-Commerce platforms owned by SMEs in Kenya in the study. This approach ensured that the entire population of interest was represented, allowing for a comprehensive understanding of the cybersecurity landscape in the context of SME-owned e-Commerce platforms. The study

adopted a purposive sampling technique to carefully identify SME entities. The study considered the appropriate study population for participation in the study.

The appropriate study population SMEs was first determined using a specific criterion, an SMEs selected based on: -

i. Active and operational e-Commerce platforms, SMEs was selected if they had an active and operational e-Commerce platform, this was research focus, the online stores.
ii. Have a well-established history of at least 3 years.

    This factor was to limit research to the SMEs which was successful or has well established business structure. This represented the success rate of an SME.
iii. More than 2,000 traffic per month,

    This factor considered the platforms with more visit as a target for cybercriminals.
iv. Revenue not less than 3million per month, this represented a SMEs with high transactions online.
v. Has employees not less than 30.

After applying these criteria, predetermined by researcher, 60 SMEs met the requirements and therefore qualified as the study population. The researcher used guidance from Cresswell's (2018) research, which suggests that a sample size of at least 10% is appropriate for research. Based on this guidance, the researcher chose a sample size that corresponded to 66.67% of the study population. As a result, 40 participants were selected to participate in the study as the sample size.

The sample size for this study was 40 SMEs, chosen using purposive sampling. Purposive sampling is a non-probability sampling technique in which the researcher deliberately selected cases based on specific criteria relevant to the research question. This sampling method was chosen because it allows for selecting specific cases that are the most informative and representative of the population of interest (Naderifar et al., 2017).

Determining the proper sample size of the research was reinforced by the principle of saturation, the letter state that the sample size is large enough if it can answer the research questions which results in achieving the study's aim. Saturation was considered to have been achieved when any further data collection did not result in the identification of a new findings that can be used for understanding and explaining the analysed findings, it occurred when no new information was received in the data collecting process and newly acquired data became redundant (Vasileiou et al., 2018; Hennink et al., 2017).

According to Weller et al. (2018) it is important to use saturation in cases where certain items, themes, and behaviours are common and widespread within a population. The study concluded that a sample size of 40 was more than enough since saturation was reached at 16th respondent. Hennink et al. (2017) discovered that qualitative studies can attain saturation using a small sample size. The findings suggested that 9-17 interviews or 4-8 focus group discussions were sufficient to reach saturation for studies with a homogeneous population and limited research objectives. Table 7 presents the distribution of the SMEs that formed the sample size.

TABLE 7: E-Commerce Target Population (Source: Research)

CATEGORY	NO. OF SMES	PERCENTAGE (%)
Cosmetics	12	30
Electronics	10	25
Fashion	6	15
General Stores	4	10
Booking	4	10
Grocery	4	10
Total	**40**	**100**

To determine the saturation, a statistical method called partial least squares regression was used. The method combines principal component analysis and linear multiple regression to identify correlations between independent and dependent variables. The empirical data was grouped into two blocks: the initial 75% and the last 25%. The saturation was determined by comparing the themes of interest (π) with the collected data (denoted by ^). The study found out that the results from the first and second blocks were similar, it was concluded that saturation had been reached. Set theory was also used to support these statistical modelling techniques by highlighting that there are infinite themes (Ω), including themes of interest (π) in the research study, and the themes collected from the empirical study (^). Saturation will be achieved when π equals ^.

The sample of 40 SMEs was chosen from a diverse range of industries and goods and services sold. The study population provided information which enabled the researcher to derive key factors that should be considered in an evaluation model, hence achievement of objective II of the study, the data allowed for a more comprehensive understanding of the current state of

cybersecurity practices within the e-Commerce industry and how an effective model can be developed.

3.5 Data Collection

The data for the study was collected using various data collections tools, including, observation-checklist, participant observation, and questionnaires, the observation-checklist was filled using output from the test cases and vulnerability scanning tools. Test cases was used to check for the presence of specific security measures, such as two-factor authentication, this was done by participant observation and testing if the 2FA is functioning using a sample account. This was done manually by signing into an e-Commerce account and verifying if a code is sent to a recovery account or a phone number attached to an account. Vulnerability scanning tools was used identify potential security vulnerabilities in the target systems, this included using OpenVAS (Open Vulnerability Assessment System), which is an open-source vulnerability scanner (Greenbone, 2021); the Metasploit Framework was used to perform penetration testing and identifying vulnerabilities (Rapid7, 2021).

The study also utilized the Greenbone Vulnerability Management (GVM), which is a security management tool, that includes vulnerability scanning, asset management, and reporting capabilities (Greenbone, 2021). SQL Map, a tool for detecting and exploiting SQL injection vulnerabilities (Bernardo, 2021), and Nikto, a web server scanner (Cope, 2021), were among tools that made the study a success. SpiderFoot, an open-source reconnaissance tool (SpiderFoot, 2021), and Intrigue, an open-source reconnaissance and threat-hunting platform (Intrigue, 2021), were employed to achieve triangulation. Maltego framework enabled the researcher to perform data

mining in the e-Commerce platforms and analyse the data into an insight that can be used to make a conclusion (Paterva, 2021), and Browser Exploitation Framework (BeEF) triangulated the data and added weight to the research data validity and reliability (BeEF, 2021).

3.6 Data Analysis

The study used both the qualitative and quantitative data analysis methods. The content analysis was used to analyse the qualitative data by examining the content of the data that was collected. The method was used to analyse the data collected using the observation checklist, test cases, and observations. The data analysis process involved coding the data into categories and determining the patterns and themes in the data. Statistical analysis was used to perform quantitative analysis by using the numerical data to determine the patterns and any relationships in the data. A number of cybersecurity tools and frameworks were used to perform data analysis, this included the GVM, Maltego, and Metasploit, which provided data mining and analysis capabilities. The threat hunting enabled the researcher to researcher to identify, find and analyse indicators of compromise in the e-Commerce. The different data analysis tools used by the researcher allowed correlation of the data from different (Eckerson, 2018). The researcher used the Maltego for data visualization.

3.7 Evaluating and Validating the Model

The model was evaluated and validated using empirical methods to ensure its validity, accuracy, and reliability. Experimental design was used to test the effectiveness of the model in a controlled environment, that is in an e-Commerce replica. A series of experiments were performed on an e-Commerce replica, an e-Commerce replica was developed for both Content Management Systems (CMS) and non-CMS e-Commerce sites, and used to test the specialized tools used to determine

the status of a certain attributes, e.g. binary evaluation of Web Application Firewall (WAF) detection, this involved installing and configuration the WAF, and testing the presence and subsequent uninstall and retest to determine if the tools accurately determined the absence of the firewall, the empirical test involved the manipulation one or more variables in the replica e-Commerce (e.g., SQL Injection, software version and Cross Scripting) and measuring the impact of these variables on the output of the model, this addressed objective number (IV). The pilot testing was done, during which the model was applied to assess the cybersecurity level of sampled SMEs, this was used to adjust the research tools to fit the research objective and fine tune tools ready for data collections. The results of the pilot testing output were analysed to assess the feasibility, usability, and acceptability of the model. The 5 independent variables were totaling to 100 points, the variables had 20 attributes, the cybersecurity level was quantified in percentage form and converted to qualitative form of 3 levels, Highly Secured if above 90 %, Critical if below 50 and Moderate between 51 and 89.

3.8 Pilot Test

The study included pilot testing on five distinct e-Commerce platforms. The goal of pilot testing was to examine and fine-tune the research methodologies, instruments, and processes prior to conducting the main study with the target population. The study carried out a pretest of five SMEs e-Commerce platform to evaluate the research tools. The pilot testing further enabled the researcher to fine tune the observation-checklist to ensure that the data collection process was capturing the valid data. The study tested the validity and reliability of the tool over time by performing the re-test and comparing the results to the pre-test refer to table 8 on Pilot Testing.

TABLE 8: Pilot Testing Results

	ACCESS CONTROL		DATA SECURITY		NETWORK SECURITY		SOFTWARE SECURITY		AUTHENTICATION & AUTHORIZATION		TOTAL MARKS	
	Pre-test	Re-test	Pre-test	Re-test	Pre-test	Re-test	Pre-test	Re-test	Pre-test	Re-test	Pre-test	Re-test
X1 1	0	0	24	23	6	6	10	10	10	10	50	49
X2 2	0	0	9	9	3	3	5	5	5	5	22	22
X3 3	0	0	5	5	3	3	3	3	5	5	16	16
X4 4	0	0	10	12	3	3	5	5	3	3	21	23
X5 5	0	0	4	4	0	0	3	3	0	0	7	7
X6 6	0	0	24	24	6	6	10	10	10	10	50	50

3.9 Validation of the Results

To determine the validity of the research instrument, the results were compared to two commonly used frameworks and standards: - Common Weakness Enumeration (CWE) and Common Vulnerability Scoring System (CVSS). CWE provides a complete list of software flaws and vulnerabilities, whereas CVSS provides a standardized approach for assessing and scoring vulnerability severity. The study improved the content validity of the observation checklist by using CWE and CVSS as standards. The observation checklist in this case was created to include the key components of cybersecurity vulnerabilities and weaknesses particular to e-Commerce platforms.

Crosschecking entailed comparing the identified vulnerabilities and weaknesses to the CWE database and assessing their severity using the CVSS scoring system as in table 10. This all-encompassing approach ensured that the observation checklist efficiently caught and addressed the known vulnerabilities and weaknesses of e-Commerce systems. The study confirmed that it covered the primary areas of concern within the domain of e-Commerce platform vulnerabilities by matching the checklist with CWE. Furthermore, using CVSS to validate the severity ratings of the detected vulnerabilities added credibility to the findings and allowed for appropriate classification and prioritization. Table 9 gives a rating score as outlined in the CVSS standards.

TABLE 9: CVSS Score (Source: CVSS, 2019)

RATING	CVSS SCORE
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10

3.10 Summary of Research Design

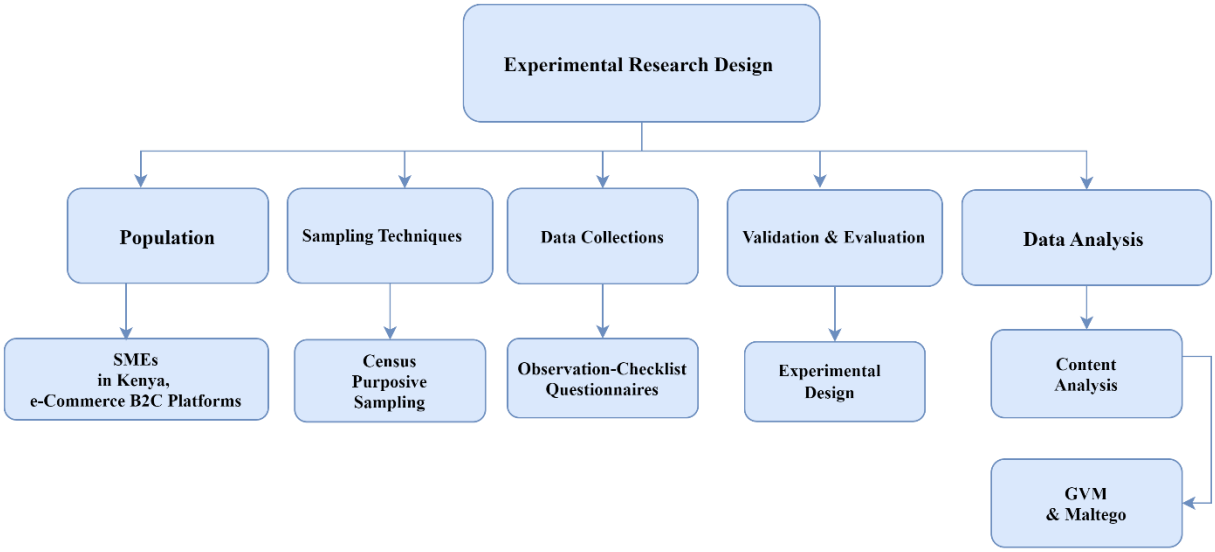
The study used a comprehensive research design to ensure data validity and reliability. Data were collected from 40 participants and reinforced with penetration testing and scanning using Kali Linux tools on 36 e-Commerce platforms. To ensure consistency, multiple scanning and practical test cases were performed Experimental tests were conducted by altering variables in e-Commerce platforms and scanning, penetration testing, test cases, and observations were performed, and the results were consistent.

In terms of data validity and reliability, the study employed several measures to ensure validity, including using of CVSS and CWE standards. The use of a sample of 40 participants from

different industry ensured comparable results. The combined use of participant observation, penetration testing and scanning, and questionnaires provided triangulation of the results. The participants were purposively sampled but also randomly identified, further strengthening the study's validity.

The researcher had technical knowledge on cybersecurity and an understanding of the e-Commerce context from the development stage to live production, the researcher had 5-year experience in developing e-Commerce, and managing on premise, shared hosting, and cloud infrastructure and hence knew what data was valid and when consistencies were not being recorded. Figure 12 summarizes the research design used in the study.

FIGURE 12 : Research Design



CHAPTER 4: DATA ANALYSIS, FINDINGS, AND DISCUSSION OF RESULTS

4.1 Introduction

The purpose of this chapter is to give the research findings, including an overview of e-Commerce cybersecurity levels among SMEs. The chapter provides a full analysis of the data collected from the SMEs, including their feedback and any vulnerability assessments performed. It is vital to note and stress that the research was carried out in a way that protected the SMEs' confidentiality and privacy. The study took all required precautions to guarantee that the SMEs' identities were not divulged in any way that could jeopardize their security or reputation and business operations. This includes coding the SMEs' rankings to safeguard their anonymity and prevent their identities from being revealed.

The study's findings on a cybersecurity assessment model for SMEs are presented in the study, which included 40 SMEs in the e-Commerce sector. All the 40 SMEs contacted responded to the questionnaires. Furthermore, the study considered e-Commerce owners' requirements for confidentiality and anonymity if a vulnerability was discovered in their e-Commerce platforms. The SMEs' rankings were coded to guarantee that their identities were not revealed, to prevent losing online customers and being viewed as less secure.

4.2 Response Return Rate

The response return rate is the percentage of questionnaires, interviews or surveys completed and returned by participants out of the total number of questionnaires given. A high response rate improves the accuracy and reliability of the data obtained and guarantees that the data is representative of the population being studied. The response rate in this research study was 100%,

suggesting that all 40 SMEs who were invited to participate completed and returned the questionnaire and follow-up oral interview. This high response rate positively indicates SMEs' engagement and interest in the e-Commerce sector. It is most likely owing to the careful attention paid to confidentiality and anonymity and the perceived relevance of cybersecurity in the e-Commerce industry. Of the 40 participants in the research, a total of 36 (90%) granted permission for their e-Commerce site to be assessed using the model developed. This assessment involved several methods, including penetration testing, test cases, scanning, and policy analysis. Table 10 shows distribution of response rate.

TABLE 10: Response Rate

CATEGORY	PARTICIPANTS	RESPONSE	PERCENTAGE
Questionnaires	40	40	100%
Assessment Via Model	40	36	90%

4.3 Demographic Information.

The research sought to identify essential demographic information such as the kind of industry represented in the e-Commerce sector and traffic to online retailers to acquire an accurate representation of the study population. According to the data collected, the cosmetic business is the most well-represented, accounting for 30% of respondents, followed by electronics at 25%, fashion at 15%, and general stores, booking sites, and grocery at 10% each. This distribution provided useful insights into the Kenyan e-Commerce ecosystem and the industry’s most likely to experience cybersecurity challenges.

The e-Commerce platforms received 3,000 visitors each month on average, underlining the potential impact of any cyber-attacks or data breaches on many customers. Figure 13 and 14 depict the user traffic received by the e-Commerce platforms operated by SMEs every month.

FIGURE 13 : Demographic Information

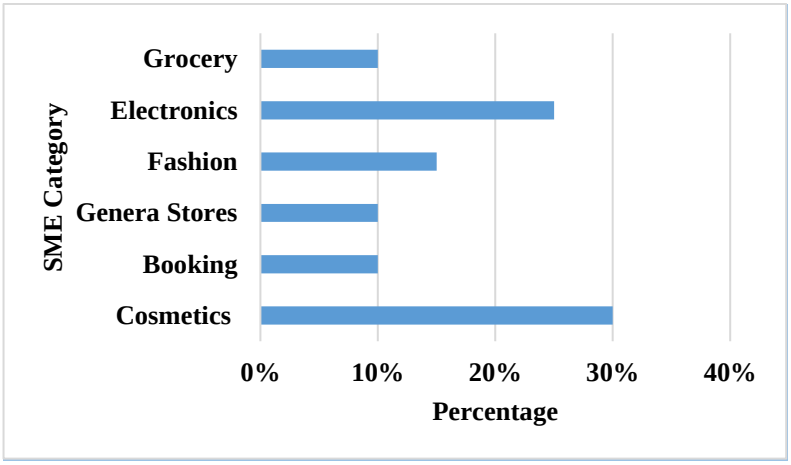
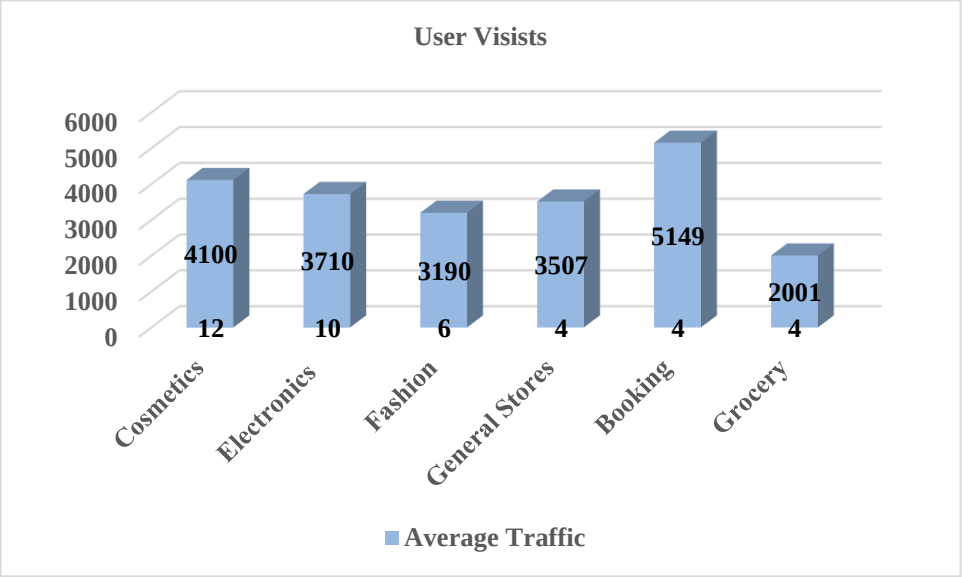


FIGURE 14 : e-Commerce Traffic



4.4 Research Findings

4.4.1 Objective One Results

The first objective of the research was to review the current state of cybersecurity assessment strategies by the SMEs and challenges experienced while running their B2C operations, to achieve this objective a combination of self-administration questionnaire and desk research was undertaken so as to deeply and accurately capture the unique needs of the SMEs. The self-administration questionnaire involved the e-Commerce owners answering a specific question concerning the B2C operations and how they apply the existing models if any in assessing the e-Commerce platforms.

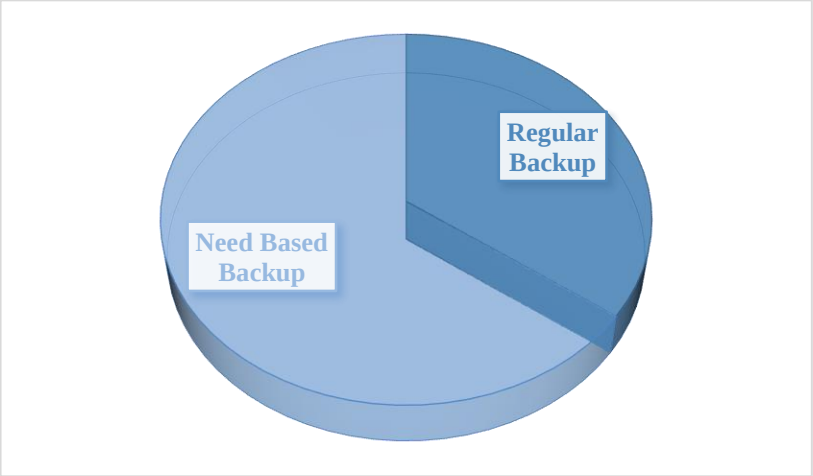
a) Cybersecurity Assessment Strategies

According to the findings of the study, 55% (22 out of 40) of e-Commerce administrators monitored user behaviour on their website and was guided by the existing standards majorly the

SMECRA model, ISO 27001, Cybersecurity Majority Model, and RiskIT model. A vast majority of these respondents indicated good security in terms of user complaints about account activity. The 45% of administrators who reported not monitoring user behaviour, on the other hand, received more user complaints about their account's activity. This emphasizes the significance of monitoring user activity as an efficient strategy to improve security and prevent future problems.

In terms of e-Commerce administrators' backup routines, the study discovered that 35% (14 out of 40) of them acknowledged taking regular backups of their e-Commerce data, this was guided by Enterprise Risk Management model and the ISO 27001. The remaining 65% (26 out of 40) just took backups when migrating to a new platform. This suggests that SMEs have taken no attempts to improve their backup policies, one of the SMECRA model strategy is frequent backups as critical factor for data recovery and business continuity in the event of system failures, data corruption, or cyber-attacks. Figure 15 shows the backup strategies implementing by the SMEs.

FIGURE 15 : Backup Practice



The study also looked at the cybersecurity training that employees and e-Commerce administrators received. The research findings were, that 45% (18 out of 40) of respondents said they did not provide any cybersecurity training. Among those who did provide training, 22.5% (9 out of 40) did it on demand, 12.5% (5 out of 40) did so once a year, and 20% (8 out of 40) did so twice a year or more. This implies that SMEs have not prioritized cybersecurity in their online operations, even though frequent cybersecurity training for employees and managers is critical, as cybersecurity threats and best practices are always evolving. Table 11, details number of training offered by SMEs to employees and administrators of e-Commerce platforms.

TABLE 11: Training Offered

NUMBER OF TRAINING	NUMBER OF SMES	PERCENTAGE
0	18	45%
1	5	12.5%
2	8	20%
3	0	0%
4 or more	0	0%
On Demand	9	22.5%
Total	**40**	**100%**

b) Industry Specific Regulations

The study found that, 85% of the 40 respondents did not mention any industry-specific cybersecurity standards, regulations or requirements for their e-Commerce platform. The General Data Protection Regulation (GDPR) was mentioned as a relevant regulation by only 15% of respondents. This indicates a lack of awareness and implementation of industry-specific cybersecurity guidelines or requirements among Kenya's e-Commerce enterprises. To protect their customers' data and keep their trust, e-Commerce enterprises must understand and comply with relevant legislation and standards.

c) Challenges faced by SMEs.

The study sought to discover the challenge that SMEs have when adopting cybersecurity in their e-Commerce platforms. The SMEs identified several significant challenges that e-Commerce enterprises in Kenya face when implementing cybersecurity measures. Budget limits, lack of cybersecurity tools to conduct security assessments, lack of awareness and expertise on cybersecurity, and insider threats were among the challenges experienced by SMEs. Budget limits was one of the major challenges since they lack the financial resources to invest in efficient cybersecurity solutions and technology. This made it difficult for them to develop comprehensive cybersecurity strategies and left them vulnerable to cyber-attacks since they rely on free cybersecurity techniques that are not reliable and efficient.

The findings of this study are in support with and corroborate the research conducted by Ngugi (2016), as well as the studies carried out by Mwangi (2021) and Satyanarayana et al., (2022).

This suggests that the results of this study are consistent with previous research, indicating that there is a convergence of conclusions drawn by different studies on the same or similar subjects.

Another key challenge is a lack of tools and resources to conduct security assessments; 100% of e-Commerce organizations examined did not have the requisite testing tools or resources to undertake complete security evaluations of their platforms. As a result, they were unable to identify and address vulnerabilities in a timely manner, leaving them vulnerable to cyber threats. Figure 16 summarizes the challenges experienced by SMEs in Kenya.

FIGURE 16 : SMEs' Challenges

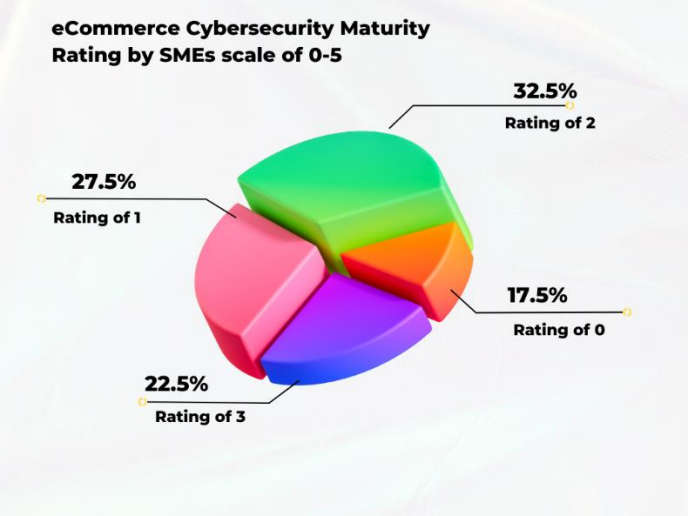
The researcher also discovered that employees and administrators have a substantial lack of awareness and skill in cybersecurity practices and risks. This is a serious concern because employees and administrators are vital to the security of e-Commerce platforms. Without sufficient training and awareness, they may accidentally expose platform's vulnerability through simple errors and configurations. The 40 SMEs contacted stated that they do not have access to an expert that can assist them in evaluating their e-Commerce.

d) SME's Cybersecurity Maturity

The research discovered that most SMEs e-Commerce were not secured, e-Commerce cybersecurity maturity rating on a scale of 0-5 showed that 17.5% rated their platform at 0 in terms of platform security meaning they had no or very minimal cybersecurity measures in place, 27.5% rated their platform at 1, indicating that they had some basic security measures in place but had not fully implemented a comprehensive cybersecurity strategy,32.5% rated their platform at 2, showing that they had implemented some cybersecurity measures but still had significant room for improvement, 22.5% rated their platform at 3, indicating that they had implemented a cybersecurity strategy, but still had some areas for improvement.

The lack of SMEs rating their platforms as 4 or 5 shows that no SMEs in Kenya have fully matured cybersecurity measures in place for their e-Commerce platforms. This is a cause for concern, as cyber threats are increasing, and SMEs are increasingly becoming targets for cybercriminals. The research concluded that SMEs in Kenya are not adequately protected against cyber threats. This puts their business and their customers at risk of cyberattacks, data breaches, and financial losses. This agrees with Muhati (2018) research, which discovered that SMEs tend to have insecure networks. Figure 17 is a graphical representation of the e-Commerce cybersecurity rating by SMEs.

FIGURE 17 : e-Commerce Ratings



4.4.2 Objective Two Results

The second objective of the research was to identify the key cybersecurity assessment factors that should be considered in an assessment model, this was achieved by analysis of base factors of existing models, standards and strategies and aligned with the challenges faced by SMEs, the factors were derived from the first objective. This objective was achieved by derivation of key variables from the existing model and adding a factor to consider the unique needs of the SMEs and the rapid evolution of cybersecurity. The study discovered a number of variables and attributes that are key to cybersecurity assessment: -

a) Access Control

Access control factor is key in determination of controls for roles-based access strategies implemented in an e-Commerce. The access control mechanism differed in each e-Commerce, 33 e-Commerce showed that new account creation is classified as a customer account this represent

98 percent of the tested e-Commerce, 3 e-Commerce set new account created by user as an author, 25 e-Commerce had four accounts and roles, administrator, shop manager, customer, and subscriber, 11 e-Commerce had custom accounts roles.

i. Brute Force Attacks

An e-Commerce should ensure an account lockout and limit the Brute forcing, this factor ensures that no user can send authentication requests that exceed a given threshold. Brute force attack was possible in 94.44% of e-Commerce platforms, the e-Commerce platforms had not implemented account lockout and had no password complexity met, 5.56% of e-Commerce platforms had implemented account lockout and had password complexity met and brute force was not possible on the platforms. The brute force attacks was tested at 3 levels and was achieved using hydra from Kali Linux tools, the test was achieved using the command: -*"hydra -L e-Commerce_users.txt -P passwordlist.txt target_e-CommerceIP ssh -t 4."* , secondly use of test cases for password lockout and third use of GVM.

ii. Access Control Bypass

The cybersecurity strategies enforce authentication and authorization mechanisms, this attribute assesses if there is any unauthorized access or vulnerability associated with access control bypass. The 36-e-Commerce tested, representing 100% had no HttpOnly Flag set to cookie, the cookie could be accessed by JavaScript. If a malicious script was to be run on the e-Commerce pages, the cookie could be accessible and could be transmitted to another site. If that was session cookie, then session hijacking may be possible in the e-Commerce platform, also the e-Commerce cookie had

been set without the secure flag, which means that the sessions cookie can be accessed via unencrypted connections, enabling attackers to take over a session.

iii. Role Escalations Access

The factor is critical in assessing the system role-based strategies in place. The 36-e-Commerce tested had no Anti-CSRF tokens in a HTML submission form found in their e-Commerce. This finding shows that an attacker can force a victim to send an HTTP request to a its destination without their intention to perform an action as the victim. The nature of the attack is that CSRF exploits the trust that an e-Commerce has for a user, this exploits an active session of an authenticated user, the 36 e-Commerce also lacked SameSite attribute, which means that the cookie can be sent because of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

iv. Privilege Escalations

The attribute evaluates the elevation of system access, permissions and access to resources. Cross Origin Resource Sharing (CORS), 20 e-Commerce (55.56%) had CORS misconfigured, this means that the web server of the affected e-Commerce allowed any third-party web applications to perform privileged actions via the web browsers of authenticated users.

b) Network Security

The network security was determined by identifying factors which can lead to exposure of the network information, in involved determining if mapping of the network was possible, any directory listing and server information leaks.

i. Network Mapping

The factor evaluates the possibility of extracting systems environment information and leakage of such information to an external user, the factor has a number of category of data exposure.

Directory Listing-Based on the data analysis of 36 e-Commerce platforms, the research found that directory listing was enabled in 18 platforms this was detected via aggressive detection and direct access with confidence level of 100%. This represents a significant number of e-Commerce websites that are vulnerable to directory traversal attacks. Directory listing is a feature of web servers that allows users to view the contents of a directory on the server. While this can be useful in some cases, it can also be a security risk if not properly configured. Directory traversal attacks occur when a hacker can access files and directories that are outside of the web server's root directory.

This can be done by manipulating the URL or by exploiting vulnerabilities in the web application. The impact of directory traversal attacks can be significant. Hackers can access sensitive data such as customer information, payment details, and other confidential data. This can result in financial loss, reputational damage, and legal issues for the e-Commerce website. "*I have never heard of Directory Listing techniques, effects or mitigations*", one of the e-Commerce administrators said when asked on the impact and mitigation of the e-Commerce directory Traversal attacks during follow-up interviews, this show concerns on the training and awareness of the administrators on the cybersecurity evolutions. The 40 e-Commerce administrators who were asked on how to mitigate the the risk of directory traversal attacks, did not come out clear most of them not highlighting the steps and basic configurations, this is affirmed by the data from

"*How many trainings do you carry out for e-Commerce platforms administrators*", 30 e-Commerce owners carried 2 per year, which is a bit not enough considering how evolution of cybersecurity attacks occurs, 5 e-Commerce said the training were on demands basis and 6 e-Commerce owner has never trained nor consulted third party on cybersecurity issues in their e-Commerce. The 40 e-Commerce administrators did not mention the access control mechanisms such as file permissions, web application firewalls, and intrusion detection systems as techniques used in managing directory listing risk.

Server Leaks Version Information-The researcher found that 23 of the 36 e-Commerce had server leaks via "Server" HTTP response Header Field, this exposed the application server information which will enables attacker to perform reconnaissance and identification of vulnerabilities, by looking for plugins and types of platforms in the systems, 6 of the e-Commerce had debug error messages which expose the hosting environment information's like IIS and Apache servers.

ii. Remote Access

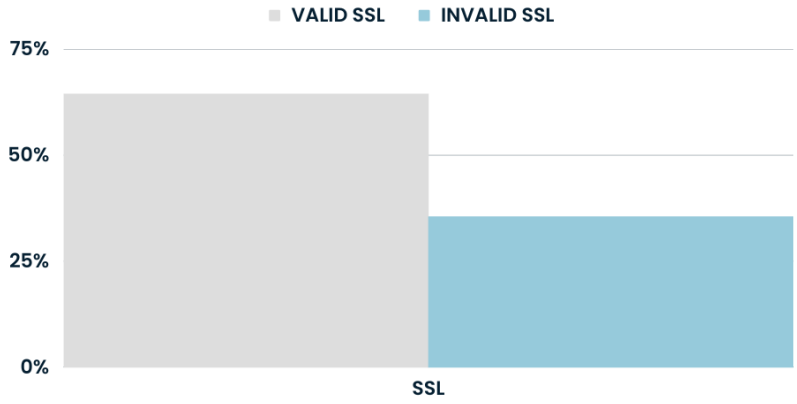
The remote access technologies were evaluated to determine how secure they were, it involved determining any vulnerabilities associated with the technologies and their impact. The assessment involved examination of the SSL: -

Secure Socket Layer (SSL)

The study findings indicated that a considerable proportion of SMEs operating e-Commerce platforms in Kenya did not utilize Secure Sockets Layer (SSL) certificates or had not appropriately implemented them or was expired. Specifically, the study identified two groups of e-Commerce

platforms: those that had valid and correctly configured SSL certificates and those that had SSL certificates that were either expired or not correctly redirecting, 11 cases, equivalent to 35.56% of the sample had invalid SSL certificate while, 25 or 64.44% of e-Commerce platforms sampled had correctly configured their SSL certificates. This observation is a concerning indication of the critical cybersecurity maturity of the SMEs and highlights the need for improved security measures to safeguard their customers' data and enhance their trust in e-Commerce platforms. The researcher found that 15 e-Commerce remote SSH servers were configured to use weak key exchange algorithm or allow the weak key exchange (KEX) algorithm like the 1024-bit MODP group and attacker can quickly break individual connections. Figure 18 shows SSL implementation of the e-Commerce platforms.

FIGURE 18 : SSL Implementation

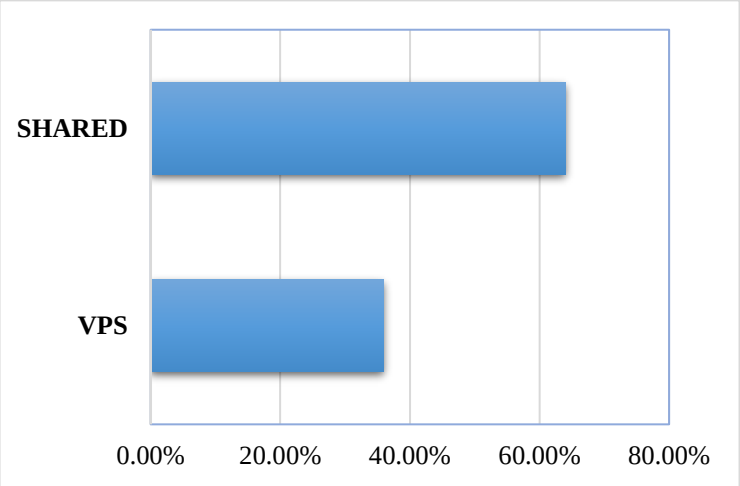


iii. Cloud Security

The research study found out that 23 e-Commerce were hosted on a shared hosting environment, and 13 were on a VPS. The research revealed that e-Commerce sites hosted on shared environments were more vulnerable to cyber-attacks due to the shared nature of resources. These sites were found to have weaker security measures in place, leaving them susceptible to various

security threats. On the other hand, e-Commerce sites hosted on VPS were found to have better security measures in place due to the level of control and customization provided by the hosting environment. Figure 19 shows the type of web hosting implemented by the SMEs.

FIGURE 19 : Cloud Implementation



iv) DoS Attacks

The e-Commerce platform was evaluated to determine presence of vulnerabilities that are associated with denial of service, and also version of ISC Bind. The assessment included: -

ISC BIND End of Life (EOL) Detection

The research sought to know the ISC BIND status of the hosting environment of the e-Commerce, 23 remote host were found to be using ISC BIND version which had reached End of Life, and which was associated with several vulnerabilities discovered in previous years, which vendors are not currently fixing it. The versions have several vulnerabilities like ISC BIND DoS Vulnerability

(CVE-2018-5743) with a CVSS score of 7.5, the vulnerability of ineffective simultaneous TCP client limiting. The outdated ISC BIND cannot limit the number of TCP clients that can be connected at any given time, the unlimited simultaneous connections can lead to DoS.

v) Port and Services

This factor evaluates the status of a number of port and services, and the impact of the status of each. The study discovered that all 36 platforms that agreed to be assessed had no open port and running services that could cause cybersecurity attacks. This is a positive finding as open ports and running services can often be exploited by attackers to gain unauthorized access to a system or network, the SMEs' platforms are able to reduce their attack surface and minimize the risk of potential cyber-attacks. This is a significant step towards a more secure online business environment.

c) Data Security

This factor evaluates the strategies for the data integrity, the system will generate accurate results if data integrity is met, this factor was of emphasis in every existing model and the model developed considered the factor. The data integrity came in varied categories;

i) SQL Injection

The study assessed the data security of the platform by determining whether the SQL injection was possible in the platform. The study discovered that from the 36 e-Commerce platforms evaluated, 14 platforms were vulnerable to SQL Injection attacks with a recording of more than three instances each. This represented an approximate of 39% of the e-Commerce platforms in the study

group that were susceptible to SQL Injection attacks. The researcher discovered that the vulnerable e-Commerce was using dynamic SQL queries, did not have input validation in place, and use of outdated software and libraries.

ii) Data Retentions and Deletion

The study determined the data retention strategies and controls in place for the platforms, the study revealed that there is lack of data retention and deletion policies among e-Commerce platforms. Out of the total 40 e-Commerce platforms examined, 31 representing 77.5% had no data retention and controls and deletion policy in place, this means the 77.5% of e-Commerce had no strategy of data security. In contrast, only 9 SMEs had implemented data retention and deletion policies, and had effective controls that facilitated users to request data deletion. *"I'm more interested in customer order satisfaction, and we have a robust system to ensure that, in relation to data deletion we have no mechanisms in place since users trust us with their data",* one of the e-Commerce strongly pointed out. To mitigate these risks, e-Commerce platforms must implement robust data retention and deletion policies that comply with relevant regulations. These policies should include functionality that allows users to request data deletion and ensure that the data is permanently deleted, with no possibility of retrieval, also the platforms should conduct regular training for their administrators to ensure that they understand the importance of these policies and how to implement them effectively.

iii) XSS Attacks

The research sought to find the XSS attacks status in the e-Commerce platforms, out of 36 platforms assessed 100% were vulnerable to XSS attacks and this is particularly concerning. XSS

attacks can be used to steal sensitive information, such as usernames and passwords, or to conduct phishing attacks that trick users into providing personal information.

iv) File Inclusion Attacks

The finding also noted that all 36 platforms 100% assessed were vulnerable to file inclusion. File inclusion vulnerabilities can allow attackers to execute arbitrary code on the server, which can result in complete control of the system. This can lead to data theft, data manipulation, and other malicious activities.

d) Software Security

The factor evaluates the status of all third-party apps used in the system, the compliance status to standards, and the versions. The assessment included sub categories: -

i) Third party Apps and Plugins

The study discovered that out of the 36 e-Commerce platforms analysed, 29 of them used Content Management Systems (CMS), with the following distribution: 15 used WordPress, 4 used Joomla, 4 used Drupal, 3 used OpenCart, and 3 used Shopify, 7 e-Commerce platforms were on custom code and not utilizing any CMS, out of the 29 e-Commerce websites using CMS, 17 were running on outdated CMS, while 12 were running on stable CMS versions. The outdated CMS versions were identified as a major vulnerability as they are more susceptible to cyberattacks due to security vulnerabilities that are not patched in outdated versions. Among the 15 WordPress-powered e-Commerce platforms, the study found that 2 to 8 plugins were outdated, which represented a vulnerability that could be exploited by cyber attackers. In contrast, the e-Commerce powered by

Joomla did not have any outdated plugins, while the ones powered by Drupal had 2 outdated plugins each.

When one of the e-Commerce developers was asked whether they monitor or enable automatic plugin update, he said,

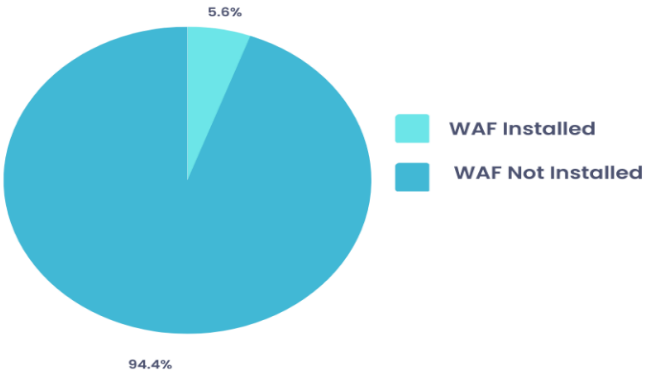
"Automatic Plugin Update can break the site since we sometimes have plugins in our site which have not gone through the WordPress Plugin Directory, so best we do it manually while checking the conflict in update." The study suggests that e-Commerce websites using CMS should update their CMS and plugins regularly to avoid being vulnerable to cyberattacks, alternatively set the plugin and CMS update on automatic mode. The e-Commerce platform should consider using stable CMS versions and plugins from reliable sources to minimize their exposure to cyber threats, since the 15 WordPress powered e-Commerce in study each had 1 or 2 plugins which are not downloaded via WordPress directory, and it means they have not been analyzed for security checks. The study also revealed that 7 e-Commerce platforms were on custom code and not utilizing any CMS. This e-Commerce was at a higher risk of cyberattacks since custom code is not usually audited regularly for security vulnerabilities. Therefore, the study recommends that e-Commerce platform on custom code should be audited regularly for security vulnerabilities and appropriate security measures put in place.

ii) Web Application Firewall

Out of the 36 e-Commerce platforms, only 2 (5.6%) had a WAF installed, while the rest (94.4%) did not have any form of firewall. The platforms that had a WAF were tested using manual

penetration testing techniques, and they were found to be effective in protecting against common web application attacks. Figure 21 shows the WAF configurations in the e-Commerce platforms.

FIGURE 20 : WAF Configurations



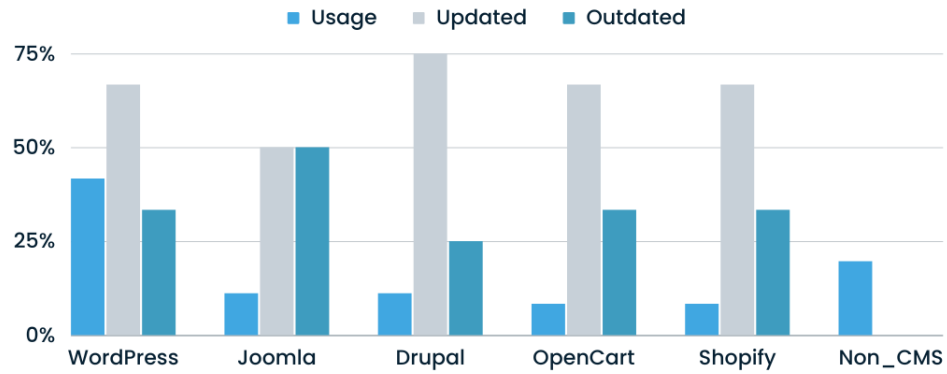
iii) Payment Gateway

The study assessed the payment gateway as a key component of the e-Commerce platforms, the payment gateway facilitate transaction for goods and service and completion of the online shopping. The payment gateway will hold the customer transaction data, this was critical and the researcher evaluated the security of payment gateways used by e-Commerce platforms for SMEs. The first step was checking if the payment gateways were listed directories of popular CMSs such as WordPress, Shopify, Drupal, Joomla, and OpenCart. The second step was checking the PCI DSS compliance status of the payment gateways. Out of the 36 e-Commerce platforms assessed, only one e-Commerce platform was using a payment gateway that was listed in the official directory of popular CMSs and met PCI DSS compliance,35 platforms were using custom payment plugins that were not in the official directories. The use of custom payment gateway poses security

to the customer data, since the custom payment plugins are not subjected to security review and the PCI DSS compliance cannot be authenticated, this study discovered that most of these plugins are subject to cyber-attacks.

The fact that only one of the custom plugins was found to be PCI DSS compliant is another major concern. PCI DSS compliance is essential for secure payment processing, and the fact that only one out of 36 payment gateways was compliant suggests that many e-Commerce platforms are not taking adequate measures to protect their customers' payment information. Figure 21 shows distribution of CMS usage and status of software and plugins used.

FIGURE 21 : Software Usage (CMS)



e) Authentications and Authorization Mechanisms

The study results showed that out of the 36 e-Commerce websites analysed, 39 had not implemented 2FA while only one had 2FA in place but was not efficient, none of the e-Commerce had Multi-Factor Authentication (MFA) in place. Two e-Commerce platforms had clear text login, which means that the login credentials were transmitted in plain text and could be intercepted by cyber attackers. This vulnerability could lead to unauthorized access to the e-Commerce website,

putting users' sensitive information at risk, the study also found that 12 e-Commerce platform did not have a user email or phone number confirmation process when creating an account. This means that users could create accounts using fictitious email addresses or phone numbers, which could be used for fraudulent activities. The research findings from the assessment of 36 e-Commerce platforms revealed that only one out of the 36 platforms had a policy in place, and only one platform met the required password complexity.

4.4.3 Objective Three Results

The third objective was focusing on the development of the model and use of the model to assess the status of the cybersecurity. The derived factors from existing models formed the base factors of the model, the model had five variables and twenty attributes, each of the five variables had specific attributes. The model has a scoring system based on the CVSS and CWE standards. The scoring system had a total of 100 points which converts to percentages. The percentages convert to qualitative output of 3 levels as demonstrated in tables 13. The model was used to evaluate the cybersecurity status of the SMEs platforms, and figure 24 shows the results of assessment. Figure 20 is a representation of the model developed for assessment of B2C e-Commerce platforms in Kenya.

FIGURE 22 : Model Developed

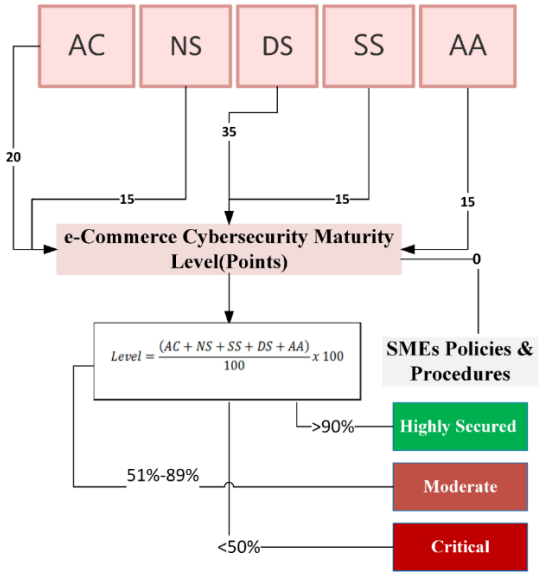
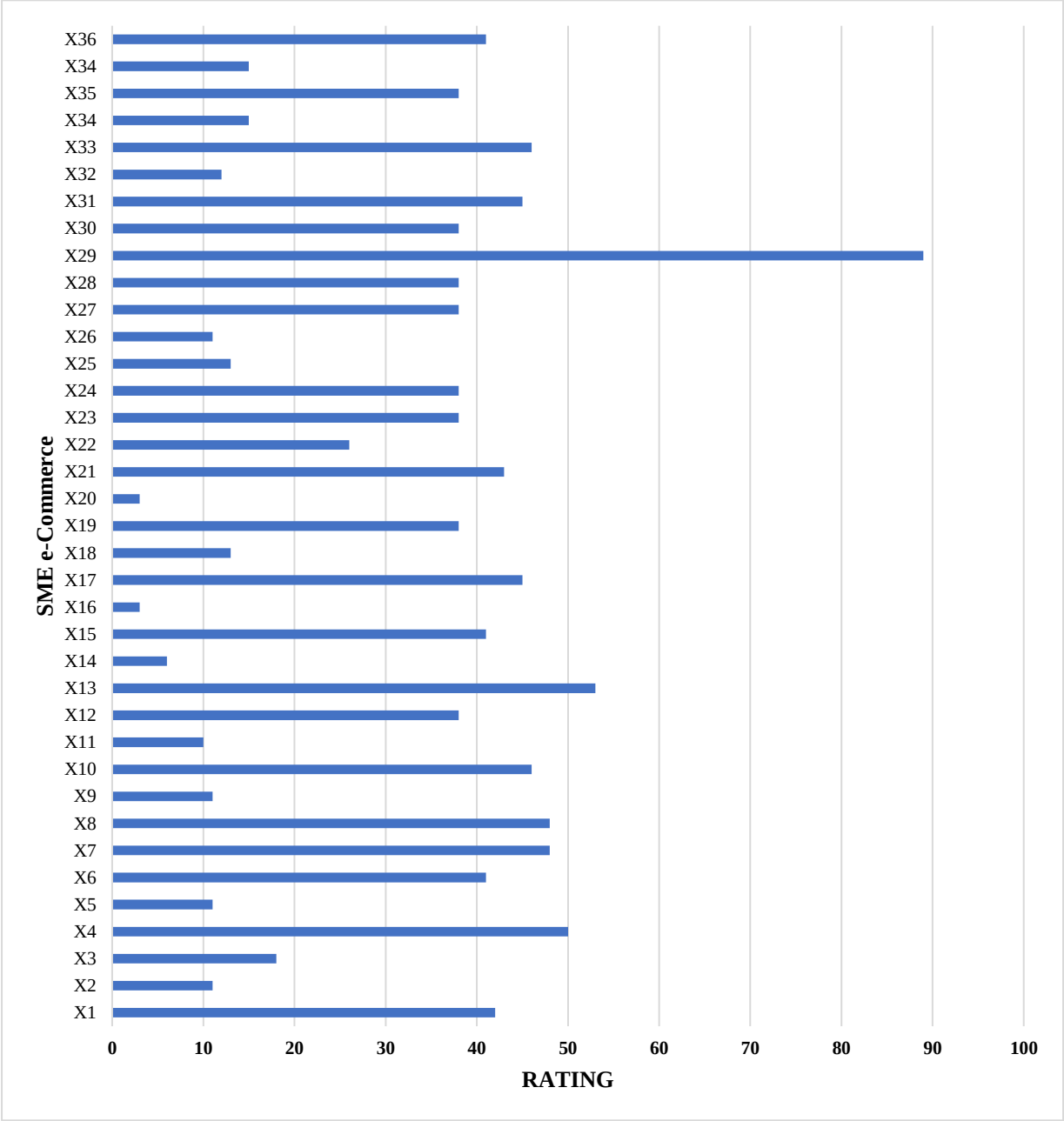


TABLE 12: Cybersecurity Assessment Rating

NO. SMES	RATING (POINTS)	CYBERSECURITY CATEGORY
2	>50	Moderate
34	<50	Critical

Figure 23 shows maturity rating for cybersecurity of e-Commerce.

FIGURE 23 : Cybersecurity Assessment -Maturity Rating



4.4.4 Discussion of Results

The study findings on e-Commerce cybersecurity status highlighted the fact that a significant proportion of SMEs running e-Commerce platforms have not implemented a secure online store, and their cybersecurity maturity level is at critical status and should not be operated online. This was demonstrated in 34 SMEs out of the 36 SMEs that were assessed, the cybersecurity status of 34 SMEs platform was recorded below 50 points, indicating a critical level of cybersecurity maturity. A critical level of cybersecurity maturity shows that the SMEs platform are vulnerable to cyber-attacks and data breaches, and will have serious implications for SMEs businesses operations and their customers. These vulnerabilities could arise from a variety of factors, including use of outdated software and libraries, the misconfiguration, weak passwords, and a lack of robust security controls, protocols and policies.

4.4.5 Objective Four Results.

The fourth objective was to validate the model, the objective was validated using experimental research design and used the CVSS and CWE standards, the study was successful in identifying a wide range of variables and factors that are required for any good cybersecurity assessment model. The study focused on five independent variables, and 20 attributes, that significantly contributed to accurate determination of the cybersecurity maturity of e-Commerce platforms. The findings emphasized the need to consider all variables to generate a comprehensive assessment of cybersecurity in the e-Commerce industry and for valid results. The model depicted that.

Access Control+ Network+ Security+ Data Security + Authentication Mechanisms + Software Security= Cybersecurity Maturity Rating/Level

CHAPTER 5: SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter gives a summary of the findings, draws inferences based on the study's findings, makes policy recommendations, future research recommendations, and discusses practical implications for Kenyan SMEs. This chapter aims to provide a complete analysis of the study's contributions to the field of cybersecurity assessment for e-Commerce platforms used by Kenyan SMEs. It begins with a summary of the research questions and objectives, followed by a discussion of the research methodology and data analysis procedures. The chapter then reviews the key findings and their implications for SMEs, as well as the limitations of the study, before closing with recommendations for future research and practical implications for Kenyan SMEs as they try improving their cybersecurity posture.

5.2 Achievement

The literature review uncovered significant cyber security concerns unique to B2C operations in Kenya. These concerns primarily revolved around the maturity of cybersecurity measures implemented in B2C e-Commerce platforms operated by SMEs in Kenya, as well as the existence of an optimal model for assessing these platforms. The review explored whether SMEs conduct thorough testing and assessment of their B2C platforms prior to their deployment for production purposes. These pressing concerns prompted the formulation of the following research question: '*What are the key cybersecurity assessment factors that should be considered in a cybersecurity assessment model?'.* To address this question, the study employed an experimental research design, aiming to empirically test and evaluate B2C platforms. The research approach involved

the observation of various test cases, enabling the investigation of the following key aspects. The study involved observation of the test cases; the research was concern with the following questions: -

i. What are the key cybersecurity assessment factors that should be considered in an assessment model?
ii. What cybersecurity challenges are faced by SMEs?
iii. How can a conceptual framework be developed for the proposed cybersecurity assessment model, including the factors, their attributes, and relationships between them?
iv. How can the model be validated?

The study identified five key factors that are key in accurately assessing the cyber security maturity of B2C e-Commerce platforms. These factors were determined to have a significant impact on the overall security of such platforms. The key factors identified include Access Control, Network Security, Software Security, Data Security, Authentication and Authorization.

The identification of the key factors of a cybersecurity assessment model led to the second research question, '*What cybersecurity challenges are faced by SMEs?'*. This was achieved by self-administration questionnaires and the study found that, *financial constraints, lack of assessment tools, expertise and hackers* were major challenges experienced by the SMEs. The third research question was, '*How can a conceptual framework be developed for the proposed cybersecurity assessment model, including the factors, their attributes, and relationships between them?'.* The study developed an optimal conceptual framework of the model by considering the

key five variables and 20 attributes. The final research question was, *'How can the model be validated?'.*

The study validated the model by use of experimental research design of test and retest and by validating the results by comparing with the CWE and CVSS standards.

5.3 Summary

There has been a rapid increase in the number of e-Commerce businesses in Kenya by SMEs, especially after the COVID-19 pandemic. However, SMEs face several challenges in operating secure online operations. These challenges include budget constraints to implement robust security measures, 40 representing 100% mentioned financial issue as one of the major constraint when they are deciding on securing their online stores, also 100% of the respondents said that they lacked expertise to implement secure online operations and also the option of hiring an external consultant is expensive, 100% of respondent mentioned tools and framework or models to assess their e-Commerce as one of the other key challenges making them use basic cybersecurity tools which has never been efficient since they get hacked frequently,100% SMEs also pointed out that there is lack of training and awareness among the shop managers monitoring the e-Commerce operations as well as contracted e-Commerce developers,85 percent of the SMEs were unaware of existing industrial regulations that guide the operations of SMEs.

The study included 40 e-Commerce SMEs, all of whom responded to the questionnaire questions, and 36 of whom agreed to have their e-Commerce examined through penetration testing and scanning. As per the research findings, the 36 SME e-Commerce platforms examined had an impressive average of more than 3,000 unique visitors each month, with active traffic daily. It is

worth mentioning that 90% of this traffic originates in Kenya, demonstrating the tremendous opportunity for SMEs to enter the local market via internet. However, with the increasing threats posed by cyber-attacks and data breaches, these SMEs must prioritize their cybersecurity posture to defend their online operations and protect their customers' sensitive information. According to the report, a large majority (85%) of the SMEs polled assessed their e-Commerce security at 2 on a scale of 0-5, suggesting that they considered their e-Commerce platforms to be insecure. It was also discovered that most of these e-Commerce enterprises ran their operations through CMS. A significant proportion (30) of the 36 e-Commerce businesses examined were rated unsecure for performing online transactions due to PCI DSS non-compliant payment gateways. These findings underscore the critical need for e-Commerce platform cybersecurity evaluations, particularly for SMEs, who may lack the funding and knowledge to deploy comprehensive security measures. Failure to address these concerns may expose companies and their consumers to cyber threats, resulting in financial losses, reputational damage, and legal consequences.

The findings of the study also revealed a multitude of security issues plaguing the e-Commerce operations of SMEs in Kenya in relation to the production environment of the e-Commerce. One of the primary concerns was the lack of a secure hosting environment, which can leave the e-Commerce platform vulnerable to cyber threats such as hacking and data breaches, a number of SMEs were hosting their platforms in a shared hosting environment and had no control of the configurations of the environment, this left the security of their platforms to the hosting providers, the SMEs reported that the Virtual Private servers and Dedicated servers were expensive and their budget do not allow migrations. The research revealed that a considerable portion of the e-Commerce 85% examined were utilizing payment gateways that did not meet the

essential security requirements of the Payment Card Industry Data Security Standard (PCI DSS). This standard provides crucial security protocols for processing payment information, and any violation of its requirements can lead to severe outcome for a business. Moreover, the study found that outdated CMS and plugins were also prevalent among the examined SMEs e-Commerce. This issue leaves their platforms open to well-known security vulnerabilities, which could be easily exploited by malicious actors seeking to gain unauthorized access to sensitive information. The study also discovered that; access control factors, including the use of weak passwords, the study discovered that platforms that were not using CMS did not meet the password requirements, no password complexity checking, multi-factor authentication (MFA) was not implemented in 35 e-Commerce platforms or two-factor authentication (2FA) was not implemented 36 platforms. These vulnerabilities pose threats to the CIA triad. The study recommends that SMEs operating e-Commerce platforms in Kenya should give a priority to cybersecurity by investing in robust security measures and ensuring compliance with the existing standards. SMEs should also seek technical expertise, training, and awareness to improve their cybersecurity posture.

5.4 Conclusion

The study assessed the cybersecurity assessment models, and standards in depth analysis, determining its extensive usage across e-Commerce. These current technology and e-Commerce adoption have played an important role in influencing cybersecurity implementation and assessment. However, these models were not expressly designed to meet the unique aspects of e-Commerce architecture. The study identified a gap in the existing literature regarding the cybersecurity assessment of e-Commerce platforms, particularly in the context of Kenyan SMEs.

This discovery underlined the crucial need for a cybersecurity maturity assessment model tailored exclusively for e-Commerce, with a focus on Kenyan SMEs.

The study was successful in identifying a wide range of variables and factors that are required for any good cybersecurity assessment model. The study focused on five independent variables, and 20 attributes, that significantly contributed to accurate determination of the cybersecurity maturity of e-Commerce platforms. The findings emphasized the need to consider all variables to generate a comprehensive assessment of cybersecurity in the e-Commerce industry. The model depicted that.

Access Control + Network + Security + Data Security + Authentication Mechanisms + Software Security = Cybersecurity Maturity Rating

The research highlights the significant potential for SMEs to tap into the local market through e-Commerce channels in Kenya, but also points out the urgent need for these businesses to prioritize their cybersecurity posture. The study reveals that SMEs face several challenges in operating secure online operations, including budget constraints, lack of expertise, and awareness of industrial regulations. Most of these CMS for their operations, which can leave their platforms vulnerable to cyber threats if not regularly updated. Outdated CMS and plugins, lack of access control measures, and non-compliant payment gateways were identified as major security issues among the examined SMEs e-Commerce platforms. The findings of the study suggest that SMEs need to invest in robust security measures, seek technical expertise and training, and comply with existing industrial regulations to improve their cybersecurity posture. A collective effort from all stakeholders, including government agencies, financial institutions, and e-Commerce platform

providers, is necessary to provide SMEs with the necessary tools and resources to operate securely online.

5.5 Contribution to Cybersecurity

The study had numerous critical contributions to cybersecurity: - firstly, the model enables SMEs running e-Commerce to identify and understand the vulnerabilities and risks that their platforms are exposed to. This identification helps SMEs to take necessary measures to mitigate the identified vulnerabilities, such as upgrading outdated software, improving access control, and addressing insecure payment gateways, by addressing these vulnerabilities, SMEs can reduce the risk of potential cyber-attacks and data breaches.

Secondly, a comprehensive cybersecurity assessment model helps e-Commerce SMEs to mitigate the impact of cyber threats by identifying potential risks and vulnerabilities before they can be exploited. This includes conducting penetration testing and vulnerability assessments, monitoring for unusual activities, and implementing robust security controls. Such measures reduce the risk of potential cyber-attacks, thus protecting SMEs against financial losses and reputational damage.

Thirdly, the model helps e-Commerce SMEs to comply with the existing industrial regulations governing their operations, implementing security measures in line with regulatory requirements, SMEs can avoid costly legal liabilities and reputational damage associated with non-compliance, a robust cybersecurity posture increases customer confidence in e-Commerce SMEs, leading to increased customer loyalty and brand reputation. The model also enables SMEs to ensure business continuity by preventing cyber-attacks that may disrupt their operations. The study

has also closed the gap in the knowledge on the intersection between Cybersecurity and e-Commerce, by identifying all the cybersecurity issues faced by SMEs e-Commerce platforms.

5.6 Research Limitations

Several limitations were discovered during the cybersecurity assessment of e-Commerce for SMEs in Kenya. One of the major constraints was access to data, which complicated the evaluation process; also, the expense of executing tests and scans on a virtual private server was a constraint. Another notable restriction was the lack of trust among SMEs, as several were hesitant to provide their data and enable third parties to complete the assessment. Furthermore, the use of Metasploit and the scanning procedure caused difficulties because several SMEs lacked the technical skills required to comprehend the extent of the assessment and hence hesitant in giving access to e-Commerce platform assessment.

Due to funding limits on dedicated servers, another limitation was the amount of test cases that could be run. Time was also a constraint, as most SMEs had to pause their operations to participate in the evaluation. To compensate, telephone follow-up interviews were done. Despite these constraints, the evaluation process was accurate and valid in answering the study questions about e-Commerce cybersecurity level for SMEs in Kenya.

5.7 Recommendations for Further Research

The study recommends research be conducted on a comparative study of cybersecurity practices among SMEs in Kenya and other developing nations in the East African region and user behaviors in online operations, to contribute to the advancement of cybersecurity in e-Commerce. This

research will highlight parallels and differences in cybersecurity practices, as well as problems and gaps in cybersecurity measures among SMEs in developing nations. The study may also make recommendations for improving the cybersecurity posture of the region's SMEs.

The study can promote information sharing among SMEs in developing countries through identifications of similarities in cybersecurity practices, SMEs in these countries can learn from each other and adopt best practices. This can contribute to a more robust cybersecurity posture for SMEs in the region.

REFERENCES

Ali, M. A., Hussin, N., Haddad, H., Al-Ramahi, N. M., Almubaydeen, T. H., & Ali, M. A. (2022). The Impact of Intellectual Capital on Dynamic Innovation Performance: An Overview of Research Methodology. *Journal of Risk and Financial Management*, *15*(10), 456. https://doi.org/10.3390/jrfm15100456

Allemang, B., Sitter, K. C., & Dimitropoulos, G. (2021). Pragmatism as a paradigm for patient-oriented research. *Health Expectations*, *25*(1), 38–47. https://doi.org/10.1111/hex.13384

Alsinawi, B. (2018). Is the NIST Cybersecurity Framework Enough to Protect Your Organization? *ISACA*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. *ITASEC*, 175–193.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzear, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Arnold, C., & Jr, S. (2022b). Cybersecurity Is Critical for all Organizations – Large and Small. *IFAC*.https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271

Bhatia, S., Behal, S., & Ahmed, I. (2018). Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions. *Versatile Cybersecurity*, 55–97. https://doi.org/10.1007/978-3-319-97643-3_3

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2021). Global Cybersecurity Index (GCI) and the Role of its 5 Pillars. *Social Indicators Research*, *159*(1), 125–143. https://doi.org/10.1007/s11205-021-02739-y

BSI Group. (2021). *ISO 27001 - Information Security Management (ISMS)*. https://www.bsigroup.com/en-GB/iso-27001-information-security/

Cash, P., Stanković, T., & Štorga, M. (2016). An Introduction to Experimental Design Research. In *Springer eBooks* (pp. 3–12). https://doi.org/10.1007/978-3-319-33781-4_1

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

Clapper, D. L., & Richmond, W. R. (2016). Small Business Compliance with PCI DSS. *Journal of Management Information and Decision Sciences, 19(1), 54*. https://www.questia.com/library/journal/1G1-459248964/small-business-compliance-with-pci-dss

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/tqm-09-2020-0202

Bernardo, D. (2021). "SQLMap - Automatic SQL Injection Tool". (2023). https://sqlmap.org/

Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment – Overview of Cyber-security legislation and implementation in SEE Countries. (2020). *Annals of Disaster Risk Sciences*, *3*(1). https://doi.org/10.51381/adrs.v3i1.45

Cope, A. (2021). "Nikto - Web Server Scanner" *Nikto2 | CIRT.net*. (2023). https://cirt.net/Nikto2

Eckerson, W. (2018). The Ultimate Guide to Embedded Analytics Keys to Product Selection and Implementation. (2023). https://www.eckerson.com/

Epstein, N. B., Falconier, M. K., & Dattilio, F. M. (2020). *Couple and family therapy across the globe: Cultural adaptations*. https://doi.org/10.1016/b978-0-12-815493-9.00016-8

European Union Agency for Cybersecurity, ENISA. (2021). Cybersecurity For SMES Challenges and Recommendations. *Http://Www.Enisa.Europa.Eu/*. Retrieved January 18, 2023, from https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Fourth International Conference on Computer Sciences and Convergence Information Technology. https://doi.org/10.1109/iccit.2009.242

Information Management Data Insights, *2*(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Ferreira, N. M. (2022). 20 Advantages and Disadvantages of E-Commerce https://www.oberlo.com/blog/20-e-Commerce-advantages-and-disadvantages

Hennink, M., Kaiser, B. N., & Marconi, V. C. (2017). Code Saturation Versus Meaning Saturation. *Qualitative Health Research*, *27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663

Horvath, I. (2022). *5 Key COBIT 5 Principles: Explained in Detail*. Invensis Learning Blog. https://www.invensislearning.com/blog/cobit-5-principles/

Intrigue (2021). Mandiant, Mandiant, Mandiant, & Mandiant. (2023). *Cyber Threat Defense Solutions | Threat Intelligence Services*. Mandiant. https://www.mandiant.com/

Išoraitė, M., & Miniotienė, N. (2018). ELECTRONIC COMMERCE: THEORY AND PRACTICE. *IJBE (Integrated Journal of Business and Economics)*, *2*(2), 73. https://doi.org/10.33019/ijbe.v2i2.78

Jain, V., Malviya, B., & Arya, S. (2021). An Overview of Electronic Commerce (e-Commerce). *Journal of Contemporary Issues in Business and Government*, *27*(3). https://doi.org/10.47750/cibg.2021.27.03.090

Kaspersky. (2023). What is Cyber Security? *Www.Kaspersky.Com*. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, *9*, 121975–121995. https://doi.org/10.1109/access.2021.3109886

Kaur, D., & Kaur, P. (2016). Empirical Analysis of Web Attacks. *Procedia Computer Science*, *78*, 298–306. https://doi.org/10.1016/j.procs.2016.02.057

Kelley, K. (2023). What is Cybersecurity and Why It is Important? *Simplilearn.Com*. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

Kotte, D., Venkatesh, R., Kumar, B., Rao, U., Kshatra, P.(2020c) Analysis of Data Breaches and Its impact on Organizations. *International Journal of Emerging Trends in Engineering Research*, *8*(10), 6989–6994.

Kravets, V. (2019). Comparative Analysis of the Cybersecurity Indices and Their Applications. *Theoretical and Applied Cybersecurity*, *1*(1). https://doi.org/10.20535/tacs.2664-29132019.1.169090

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Magnusson, A. (2022). *ISO 27001 vs. 27002 vs. 27003: What's the Difference?* https://www.strongdm.com/blog/iso-27001-vs-27002-vs-27003

Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance. *Applied Sciences*, *12*(21), 11174. https://doi.org/10.3390/app122111174

Maseko, L., & Marx, B. (2016). An analysis of COBIT 5 as a framework for the implementation of it governance with reference to King III. *Risk Governance and Control: Financial Markets and Institutions*, *6*(1), 20–34. https://doi.org/10.22495/rgcv6i1art3

Mcleod, S., PhD. (2023). Experimental Design: Types, Examples & Methods. *Simply Psychology*. https://www.simplypsychology.org/experimental-designs.html

Moturi, C., & Ogoti, G. (2020). Strengthening technology risk management in mobile money lending. *International Journal of Financial Services Management*, *10*(3), 217. https://doi.org/10.1504/ijfsm.2020.111105

Mwangi, K. (2021). Dimension Data eyes SMEs with cybersecurity service hub. *Business Daily*. https://www.businessdailyafrica.com/bd/corporate/technology/dimension-data-eyes-smes-cybersecurity-service-hub-3614606

Mthiyane, Z. Z. F., Van Der Poll, H. M., & Tshehla, M. F. (2022). A Framework for Risk Management in Small Medium Enterprises in Developing Countries. *Risks*, *10*(9), 173. https://doi.org/10.3390/risks10090173

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research. (3) 14. https://doi.org/10.5812/sdme.67670

Nagata, T., Ito, D., Nagata, M., Fujimoto, A., Ito, R., Odagami, K., Kajiki, S., Uehara, M., Oyama, I., Dohi, S., Fujino, Y., & Mori, K. (2021). Anticipated health effects and proposed countermeasures following the immediate introduction of telework in response to the spread of COVID-19: The findings of a rapid health impact assessment in Japan. *Journal of Occupational Health*, *63*(1).

Namunwa, K. (2021). Kenyan SMEs Suffering the Most From Cyber Security Threats. *CIO Africa*. https://cioafrica.co/kenyan-smes-suffering-the-most-from-cyber-security-threats/

NIST (2023). *Cybersecurity Framework*. https://www.nist.gov/cyberframework

Paterva (2021). "Maltego - Open-Source Intelligence & Forensics Tool". Retrieved from *Homepage*. (2023). Maltego. https://www.maltego.com/

Pawar, S., & Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for Small and Medium Enterprises (SMEs).

PCI Security Standards Council. (2022). *Publishes Version 1.2 of the Secure Software Standard and Program*. https://www.pcisecuritystandards.org/about_us/press_releases/pci-security-standards-council-publishes-version-1-2-of-the-secure-software-standard-and-program/

Rapid7 (2021). "Metasploit Framework: Advanced Penetration Testing Software". Retrieved from (2023). Metasploit. https://www.metasploit.com

Rosa, R. (2020). Do you know what was the first online transaction? https://www.orienteed.com/en/do-you-know-what-wasthe-first-online-transaction

Ramadhan, N., & Rose, U. (2022). Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs.

Satyanarayana, K., Chandrashekar, D., Sukumar, A., & Jafari-Sadeghi, V. (2022). How does international entrepreneurial orientation influence firms' internationalization? An exploration with Indian software product top management teams. *International Journal of Entrepreneurial Behavior &Amp; Research*, *28*(7), 1702–1731. https://doi.org/10.1108/ijebr-07-2021-0530

Sheridan, K. (2020). Phishing Campaign Targets 200M Microsoft 365 Accounts. *Dark Reading*. https://www.darkreading.com/threat-intelligence/phishing-campaign-targets-200m-microsoft-365-accounts

Shi, J., Li, R., & Hou, W. (2020). A Mechanism to Resolve the Unauthorized Access Vulnerability Caused by Permission Delegation in Blockchain-Based Access Control. *IEEE Access*, *8*, 156027–156042. https://doi.org/10.1109/access.2020.3018783

Sassower, R. (2017). Causality and Correlation. *The Wiley-Blackwell Encyclopedia of Social Theory*, 1–4. https://doi.org/10.1002/9781118430873.est0585

Seaman, J. (2020). PCI DSS Applicability. *PCI DSS*, 195–211. https://doi.org/10.1007/978-1-4842-5808-8_7

Simplilearn. (2022b). What is a Cyber Security Framework: Types, Benefits, and Best Practices. *Simplilearn.Com*. https://www.simplilearn.com/what-is-a-cyber-security-framework-article

Singh, R., Chandrashekar, D., Subrahmanya, M. B., Sukumar, A., & Jafari-Sadeghi, V. (2022). Network cooperation and economic performance of SMEs: Direct and mediating impacts of innovation and internationalization. *Journal of Business Research*, *148*, 116–130. https://doi.org/10.1016/j.jbusres.2022.04.032

SpiderFoot. (2022). "SpiderFoot - Open-Source Intelligence & Reconnaissance Tool". Retrieved from Home. https://www.SpiderFoot.net/

Statista. (2021). *e-Commerce - Kenya | Statista Market Forecast*. https://www.statista.com/outlook/dmo/e-Commerce/kenya

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225. https://doi.org/10.30630/joiv.4.4.482

Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*. https://doi.org/10.1111/risa.14092

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers &Amp; Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tamplin, T. (2023). Business-to-Consumer (B2C) | Meaning, Types, Pros, & Cons. *Finance Strategist*. https://www.financestrategists.com/financial-advisor/b2b-vs-b2c/b2c/

Terra, J. (2023). What is Client-Server Architecture? Everything You Should Know. *Simplilearn.Com*. https://www.simplilearn.com/what-is-client-server-architecture-article

Wikipedia contributors. (2023, January 10). *Payment Card Industry Data Security Standard*. Wikipedia. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Wong, L. H., Hurbean, L., Davison, R. M., Ou, C. X., & Muntean, M. (2022). Working around inadequate information systems in the workplace: An empirical study in Romania. *International Journal of Information Management*, *64*, 102471. https://doi.org/10.1016/j.ijinfomgt.2022.102471

Weller, S. C., Vickers, B., Bernard, H. R., Blackburn, A., Borgatti, S. P., Gravlee, C. C., & Johnson, J. A. (2018). Open-ended interview questions and saturation. *PLOS ONE*, *13*(6), e0198606. https://doi.org/10.1371/journal.pone.0198606

Vasileiou, K., Barnett, J., Thorpe, S. J., & Young, T. (2018). Characterizing and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, *18*(1). https://doi.org/10.1186/s12874-018-0594-7

Zande, J. V. (2022). What is e-Commerce? Definition, benefits, examples. *The Future of Commerce*. https://www.the-future-of-commerce.com/2020/01/19/what-is-e-Commerce-definition-examples/

Zubair, A. M. (2023). Experimental Research Design-types & process. *ResearchGate*. https://www.researchgate.net/publication/367044021_Experimental_Research_Design-types_process

APPENDIX I: CYBERSECURITY ASSESSEMENTOBSERVATION CHECKLIST

VARIABLES	ATTRIBUTES	SCORING MATRIX	MAX SCORE
Access Control	Privilege Escalations	3- (Number of Vulnerabilities)	±20
	Role Escalations	3- (Number of Vulnerabilities)	
	Brute Force Attacks	3- (Number of Vulnerabilities)	
	Access Control Bypass	3- (Number of Vulnerabilities)	
Network Security	Network Mapping	3-(Number of Vulnerabilities) Binary Evaluation for(Network Mapping (Pathname to a Restricted Directory, Directory Listing)	±15
	Port and Services	3-(Number of Vulnerabilities) Binary Evaluation for Open Port and Services	
	DoS Attacks	3-(Number of Vulnerabilities)	
	Remote Access	3-(Number of Vulnerabilities)	
	Cloud Security	3-(Number of Vulnerabilities)	
Data Security	SQL Injection	Binary Evaluation (±15)	±35
	Cross-Site Scripting	4- (Number of Vulnerabilities)	
	File Inclusion	4- (Number of Vulnerabilities)	
	Data Leakage	4- (Number of Vulnerabilities)	
	Data Retention	Binary Evaluation (±5)	
Software Security	Web Application Firewall	Binary Evaluation ±5	±15
	Third-Party Apps	5-(No of outdated Apps)	
	Payment Gateway	PCI compliance ±5	
Authentication and Authorization	Authentications Mechanisms.	5- (Number of Vulnerabilities)	±15
	Authorization Checking	5- (Number of Vulnerabilities)	

	Password Policy	5- (Number of Vulnerabilities) Binary Evaluation of Password Policy ±5	
Totals			±100

APPENDIX II: SELF ADMINITRATION SMES QUESTIONNAIRE GUIDE

SME Code: …….…… Category: …….……

Role: …….

Does your SME have a cybersecurity policy in place for your e-Commerce platform?

- Yes
- No

How do you manage and monitor network traffic and user activity on your e-Commerce platform?

- Yes
- No

Do you have a backup for your e-Commerce platform?

- Yes
- No

Have you ever conducted a security audit or vulnerability assessment of your e-Commerce platform? If so, what were the results?

Do you educate and train your employees on cybersecurity best practices for your e-Commerce platform?

- Yes
- No

Are you aware of any industry-specific cybersecurity regulations or standards for your e-Commerce platform? If Any state

---

State key challenges you experience in implementing cybersecurity in your e-Commerce platform.

Select policies in place.

i. Data Retention Policy
ii. Data Privacy Policy
iii. Password Policy
iv. Access Control Policy
v. Employee Training and Awareness Policy
vi. Backup and Recovery Policy
vii. Third-Party Policy
viii. Data Encryption Policy

On a scale of 1 to 5, how would you rate your SME's cybersecurity maturity for your e-Commerce platform? Where 1 is less secured and 5 is strongly secured.

On a scale of 1 to 5, rate how each of the following factor impact cybersecurity implementation on your e-Commerce platform.

i. Amount of Customer Data Collected
ii. Limited Expertise
iii. Third-Party Vendors
iv. Cybersecurity Expertise
v. Lack of Awareness
vi. Lack of Resources
vii. Complexity of Solutions

Allow analysis of your e-Commerce platform for cybersecurity posture and get recommendations on where you should improve.

- Yes
- No

APPENDIX III: KCA UNIVERSITY DATA COLLECTION PERMIT

Thika Road, Ruaraka
P.O. Box 56808-00200 Nairobi Kenya
Pilot Line: +254 20 8070408/9

Tel: +254 20 3537842
Fax: +254 20 8561077
Mobile: +254 734 888022, 710 888022
Email: kca@kca.ac.ke
Website: www.kca.ac.ke

SCHOOL OF GRADUATE STUDIES

KCA/SGS/March. 23/1 28th March 2023

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

RE: KIBET SANG REG NO: 21/02300

It is my distinct pleasure to introduce to you Mr. Kibet Sang who is a student in our institution pursuing a Master of Science in Information Systems Management in the School of Technology

Kibet is conducting a research on a topic titled: ***"Cybersecurity Index Assessment Framework: A Case of Small and Medium Enterprises (SMEs) e-Commerce Platforms"*** which is part of the requirements of the program he is pursuing. The research as well as the data procured thereof shall be used for academic purposes only.

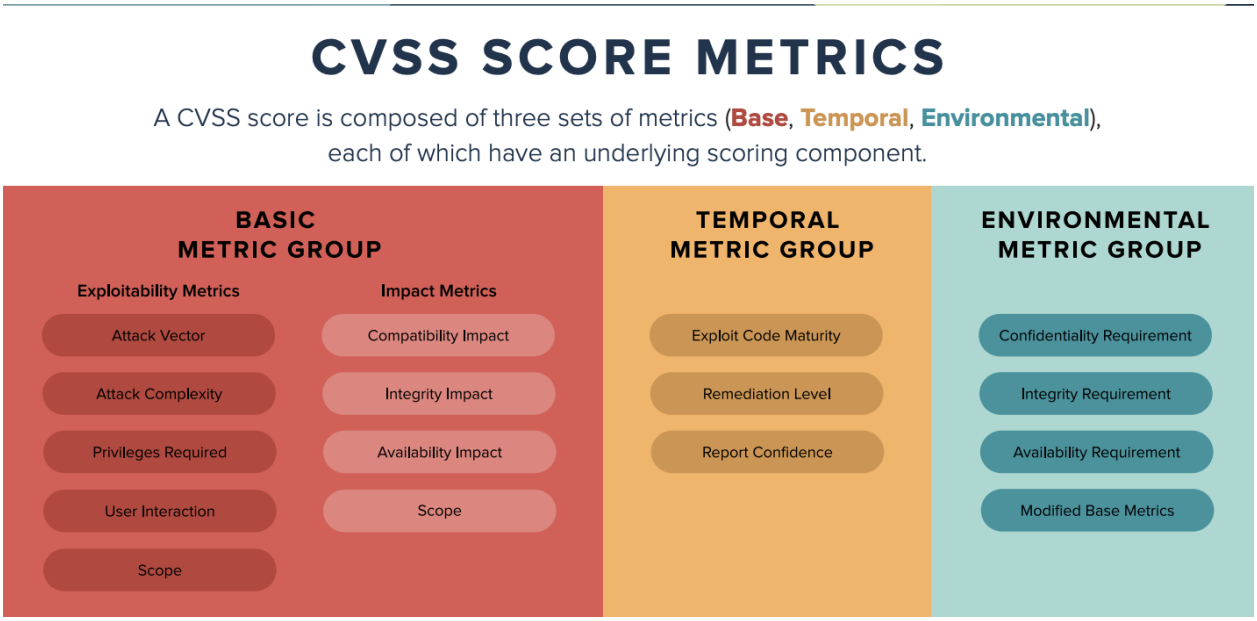
Any assistance accorded to him is highly appreciated.

In case of further inquiry, do not hesitate to contact the undersigned.

Yours faithfully,

Dr. Jackson Ndolo
Dean, School of Graduate Studies

APPENDIX IV: CVSS SCORE METRICS



APPENDIX V: VARIABLE, COMMON WEAKNESS ENUMERATION (CWE) SCORE METRICS

VARIABLES	ATTRIBUTE INDICATORS
Access Control	– CWE-284: Improper Access Control – CWE-285 CWE-287: Improper Authorization – CWE-288: Authentication Bypass Using an Alternate Path or Channel – CWE-289: Authentication Bypass by Spoofing – CWE-290: Authentication Bypass by Assumed-Immutable Data – CWE-292: Authentication Bypass by Capture-replay – CWE-293: Authentication Bypass by User-Supplied Key – CWE-294: Authentication Bypass by Capture-replay of Request – CWE-298: Improper Access Control of Functionality and Information – CWE-300: Channel Accessible by Non-Endpoint ('Man-in-the-Middle')
Network Security	– CWE-200: Information Exposure: – CWE-295: Improper Certificate Validation – CWE-296: Improperly Restricting URL Access – CWE-307: Improper Restriction of Excessive Authentication Attempts. – CWE-311: Missing Encryption of Sensitive Data. – CWE-312, CWE-319: Cleartext Storage of Sensitive Information – CWE-327: Use of a Broken or Risky Cryptographic Algorithm – CWE-297: Directory Listing
Data Security	– CWE-89 and CWE-912, CWE-913, CWE-919: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'): validate user input, which can lead to the injection of malicious SQL code into a web application. – CWE-564: SQL Injection – CWE-891: SQL Injection in a Web Application Framework: – CWE-312: Cleartext Storage of Sensitive Information
Software Security	– CWE-119: Memory Buffer: – CWE-120: Buffer Copy without Checking Size of Input (– CWE-121: Stack-based Buffer Overflow: – CWE-122: Heap-based Buffer Overflow:

	– CWE-191: Integer Underflow – CWE-194: Integer Overflow or Wraparound: – CWE-197: Numeric Truncation Error: – CWE-200: Information Exposure: – CWE-295: Improper Certificate Validation:
Authentication and Authorization	– CWE-287: Improper Authentication: – CWE-288: Authentication Bypass Using an Alternate Path or Channel – CWE-289: Authentication Bypass by Spoofing: – CWE-290: Authentication Bypass by Assumed-Immutable Data – CWE-291, CWE-308: Reliance on a Single Factor Authentication – CWE-306: Missing Authentication for Critical Function – CWE-307: Improper Restriction of Excessive Authentication Attempts