UNIVERSITY OF ZIMBABWE

FACULTY OF COMMERCE

GRADUATE SCHOOL OF MANAGEMENT

Operational Risk Management: An empirical analysis on the impact of cyber risk management on corporate performance of SMEs operating in Zimbabwe.

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE MASTER DEGREE IN BUSINESS ADMINISTRATION

BY

STUDENT NAME:	**BRIGHTON GANDA (R027875E)**
SUBMISSION DATE:	**23 March 2020**
SUPERVISOR:	**DR. A. BARA**

DISSERTATION TITLE					
Operational Risk Management: An empirical analysis on the impact of cyber risk management on corporate performance of SMEs operating in Zimbabwe.					
DISSERTATION METHODOLOGY (please tick one)					
QUANTITATIVE	✓	**QUALITATIVE**		**MIXED METHODS**	

INTAKE (YEAR AND MONTH)	
2017	**August**
REGISTRATION NO.:	**STUDENT NAME:**
R027875E	**Brighton Ganda**
DISSERTATION SUBMISSION DEADLINE	**SUBMISSION DATE**
March 27, 2020	**March 23, 2020**

This statement should be completed and signed by the student producing the dissertation.

Declaration and Statement of Authorship:

1. I hold a copy of this dissertation, which can be produced if the original is lost/damaged.
2. This work may be reproduced, communicated, compared and archived for the purpose of detecting plagiarism.
3. I give permission for a copy of my marked work to be retained by the Graduate School of Management for review and comparison, including review by external examiners.

I understand that:

4. Plagiarism is the presentation of the work, idea or creation of another person as though it is your own. It is considered cheating and is a very serious academic offence that may lead up to expulsion from the program. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited.
5. Enabling plagiarism is the act of assisting or allowing another person to plagiarise or to copy your work.

Last Name	First Name	Signature
Ganda	**Brighton**	

DECLARATION

I, ***Brighton Ganda***, do hereby declare that this dissertation is the result of my own investigation and research, except to the extent indicated in the Acknowledgements, References and by comments included in the body of the report, and that it has not been submitted in part or in full for any other degree to any other university.

…………………………………………………………..	…..……./……./…….
Student signature	Date

DEDICATION

To my late parents, Mr. and Mrs Ganda, I dedicated this dissertation. You engraved in me solid values which I always carry within my heart, and continue to guide my behaviour. You are always loved and may your dear souls rest in peace.

ACKNOWLEDGEMENTS

My gratitude and appreciation go to everyone who spared their time and willingness to assist in this research, especially those in organisation of focus, who disclosed their valuable and proprietary information used for this paper. Furthermore, I extend my appreciation to my supervisor, Dr Bara for his support and guidance throughout the entire research process.

To the most lively and intellectually astute Group, "*Group 7*," comprising Lorence Muchenje, Clifmore Chigumira, Tendai Matakanure, Kudzai Muchemwa, Ruth Soko, Sandra Mabaye, Nobert Nyahwema, Angela Muchenje and Wedzero Goredema, I say thank you for the intellectual support during the three years we have journeyed together.

A very special gratitude goes to my beloved family; my wife, Angeline and sons Tadiswa and Idris for giving me the space and time in pursuit of the MBA programme.

To God be all the Glory.

ABSTRACT

Our modern societies are now driven by technology. While this has brought about a number of advantages, the adoption of technology is not without its challenges. The widespread adoption of technology by businesses has resulted in the emergence of cyber risk. The ubiquitous interconnectivity of operations within the business and also with external parties provides the primary conduit for exploiting cyber risk vulnerabilities on a widespread basis.

This study sought to investigate the impact of cyber risk management on corporate performance of SMEs operating in Zimbabwe, a sector most exposed to cyber risk, albeit least researched. The study employed a quantitative methodology. Data were collected through structured self-administered questionnaires which were distributed through stratified random sampling of 250 respondents. From the total of 250 questionnaires distributed, 207 valid responses were obtained giving a response rate of 82.8%. The study found positive and significant relationships between the four cyber risk management constructs and corporate performance. Specifically, the study highlights that cyber risk governance, assessment practices, reduction, and awareness and training positively impacts corporate performance. These finding further enhance our understanding of the impact of cyber risk (growing phenomenon) on corporate performance, in a sector which is becoming a key growth driver for the Zimbabwean economy. It is concluded that good cyber risk management practices tends to boost business performance hence business owners and management should build robust cyber risk management practices in their companies. Furthermore, SMEs were urged to embrace rather fear the digital technology, at the same time ensure sound cyber risk management structures are in place through risk governance, assessment of the inherent cyber risk, risk reduction, and cyber risk awareness and training.

Keywords: Cyber Risk, Small and Medium Enterprises, Cyber Risk Governance, Cyber Risk Assessment, Cyber Risk Reduction, Cyber Risk Awareness and Training

TABLE OF CONTENTS

Chapter 1: Introduction

1.1. Introduction

In today’s digitally interconnected environment, every company is now a tech company. The use of digital technologies, devices and media have brought great threats to businesses, in proportional measure they bring benefits, and offer enormous opportunities. Embracing digital technology poses digital or “cyber” risk, an emergent business risk for all starts ups and small to medium enterprises (KPMG Risk report, 2014). The area of cyber or digital risk management has gained momentum in recent times and is increasingly considered an important element in the performance and value creation process of a 21st century entity. Cyber risk is increasingly becoming highly prominent with emergent corporates and SMEs, globally, and Zimbabwe included.

The economic dynamics in Zimbabwe has seen the emergence of new players on the economic front, i.e. Small to Medium Enterprises (SMEs). These SMEs are not the usual informal, backyard type of companies. Instead, these are highly formalised corporates employing up to 100 employees (SEDCO, 2010). According to the US State of Cybercrime Survey (2013), SMEs are unknowingly increasing their cyber-attack threats that increase vulnerabilities by adopting various means of IT. The most common information technology (IT) vulnerability trends include social collaboration, expanded use of mobile devices, moving the storage of information to the cloud, digitising sensitive information and embracing workforce mobility alternatives (ibid).

Various terms are used somewhat synonymously with cyber risk, including IT risk and technology risk. Eling and Schnell (2016) defined Cyber risk as risk that can undermine the integrity, availability, or confidentiality of services or data, which arise from use of IT. Furthermore, the Institute of Risk Management defines Cyber risk as any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

To date, efforts to evaluate the complexity of cyber risk have been piecemeal and uncoordinated – not unlike other emergent fields. In addition, whilst various studies have been done to assess the impact of general risk management on corporate performance and value creation (Beasley, Pagach and Warr, 2007; Hoyt and Liebenberg, 2011; Ping and Muthuveloo, 2012; Naciye, 2015; Jenya and Sandada, 2017), the outputs have been mixed and inconclusive (Kraus and Lechner 2012; Kopia et al, 2017).

As such, despite the importance of the SME sector in this country and the risk management challenges faced, cyber risk management by SMEs has received limited attention with most research work focusing on banks, pension funds and other financial services entities. There is no evidence to empirically analyse the relationship between operational risk management, particularly cyber risk, and SME performance.

The section which follows outlines the study background on the status of SMEs in Zimbabwe and operational risk management, with specific focus on cyber risk management. The chapter also covered the statement of the problem, research objectives, research questions, significance of the study together with the scope of the study. Further section of this chapter present brief review of literature related to operational risk management, the research methodology, ethical issues and an action plan.

1.2. Study Background

Growth and sustainability of SMEs has been a subject of debate between policymakers, researchers and other stakeholders globally. The debate is fuelled by the important role that SMEs continue to play in the private sector across the globe and includes employment creation (Ayyagari et al. 2016; Naude & Chiweshe 2017). SMEs are the main engine responsible for the growth of a country's economy (Kilic & Uyar, 2017; Agwu & Emeti, 2014, Siam & Rahahleh, 2010; Albu & Klimczak, 2017). According to the RBZ (2017), there are over 60,000 registered SMEs in Zimbabwe, contributing approximately 60% of Gross Domestic Product (GDP).

Locally, the survey by Finmark Trust indicated the existence of over 3.5 million SMEs in Zimbabwe. It is further reported that $3, 3 billion is circulating in the informal sector, whose main participants are SMEs (RBZ, 2015). Despite the important role played by SMEs, they continue to face a number of operational risks. Coupled by the limited resources available to mitigate these risks, the survival rate of SMEs and entrepreneurial activity is low in developing countries (Global Entrepreneurship Monitor, 2014).

Cybers risks are growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The World Economic Forum (The Global Risks Report, 2018) highlights that the financial impact of cybersecurity breaches is rising, with a growing trend towards targeting critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning. Despite the threats posed by cyber risk, only a few organisations are confident in their ability to manage the risk of a cyber attack, despite viewing cyber security as a top risk management priority (Marsh and Microsoft Corp, 2018).

According to the Reserve Bank of Zimbabwe (RBZ, 2015), cybercrime is listed as one of the crimes contributing to the US$1,8 billion estimated illicit proceeds generated from criminal activity annually in Zimbabwe. Between 2011 and 2015, about 140 cases of cybercrimes were reported and these include; Phishing (20); Credit Card Fraud (13); Identity Theft (10); Unauthorized Access (24); Hacking (72); and Telecommunications Piracy (1). These statistics are evidence of Zimbabwe's vulnerability to computer and cyber risk which in most instance cause a huge disruption to operational effectiveness of corporates.

It is apparent from the above background that SMEs at the least prepared to deal with operational challenges brought about by cyber risk, which impact their survival statistics. In addition, there is limited research done to understand the impact of cyber risk management in this regard. It was therefore important that a study be undertaken to investigate the state of operational risk management, in particular cyber risk practices in SMEs in Zimbabwe and so investigate its impact on the performance of the industry.

1.3. Statement of the Problem

Notwithstanding their potential to immensely contribute to the economy, SMEs in Zimbabwe are still faced with a plethora of operational risk issues that hinder their growth (Kwaramba, 2017). According to Risk.net, cyber risk ranks first on the top 10 operational risks of 2017, faced by corporates, including SMEs. Cyber risk is coming on board not due to the fact that SMEs have adopted significant automation in their processes, but due to the fact that there is now increased interface between the operations of the SMEs and technology e.g. e-procurement, automated payment platforms, cloud services and implementation of IT solutions across departments.

For SMEs, cyber risk is a growing concern. High dependency on information technologies and internet has opened the door to numerous vulnerabilities and cybercrime. Unfortunately, cyber risk management is often neglected within the SME environment. Recently, failure by the Ecocash payment platform resulted in lost business especially for SMEs who have come to depend upon Ecocash as the principal mode of payment. The reality for SMEs is that they must deal with a similar level of risk to their larger enterprise counterparts, but with lower budgets and limited resources.

Most large businesses have already incorporated cyber risk management into their business strategy because there is a broader awareness of the need for holistic and thoughtful protection from cyber threats (Insurance Journal, 2018). However, unlike large businesses, SMEs generally do not regard cyber risk as a strategic component in their business model despite the fact that cyber risk for SMEs is a real and growing phenomenon.

1.4. Research Aim and Objectives

The main objective of this research was to understand how cyber risk shapes and fits into the overall risk management structure thereby leading to improved shareholder value and business performance of SMEs.

This broad objective was supported by following specific objectives seeking to assess the impact of cyber risk on performance;

a) *To investigate the key factors for effective risk management in the context of cyber risk*
b) *To examine the extent to which cyber risk has impacted on company performance*
c) *Establishing whether cyber risk severity depends on firm size*
d) *Establishing the effect of effective cyber risk management on firm performance*

1.5. Research Questions

The main research question that we sought to answer was;

To what extend does cyber risk shapes and fits into the overall risk management structure thereby leading to improved shareholder value and business performance of SMEs

The main research question was addressed through the following sub questions;

a) *What are the key factors for effective risk management in the context of cyber risk?*
b) *How has cyber risk affected performance of SMEs locally?*
c) *Can cyber risk exposure severity depend on the size of the SME?*
d) *What is the impact of effective cyber risk management on SME performance?*

1.6. Research Hypothesis

The research sought to test the following hypothesis:

- *H1: Cyber risk governance positively and significantly impacts business performance*
- *H2: Cyber risk assessment practices positively and significantly impacts business performance*
- *H3: Cyber risk reduction practices positively and significantly impacts business performance*
- *H4: Cyber risk awareness and training positively and significantly impacts business performance*

1.7. Justification/Rationale or Significance of Research

The study contributed to cyber risk management by investigating its importance in the corporate performance and sustainability of SMEs. The study covered operational risk management practices in an effort to understand cyber risk management practices and the impact on SME performance. In a Volatile, Uncertain, Complex and Ambiguous (VUCA) environment, operational cyber risk identification, monitoring and mitigation is important. However, equally so important is the need for agility and relevant cyber risk management capabilities built into organisational decision-making systems of SMEs. By unpacking of the state of cyber risk management among SMEs, the study further developed a risk maturity index and fit for purpose cyber risk management framework for use by SMEs.

Research on risk management studies revealed a particular bias towards financial institution (i.e. banks) risk management. Limited attention has been afforded to risk management beyond banks, let alone risk management in SMEs. The few researches done have focused on the broader risk management which is why it is rare to find focused cyber risk management studies on SMEs.

The study therefore investigated the impact of cyber risk management on corporate performance of SMEs, results of which provided key strategic pointers on risk to owners, finance and chief executive officers of SMEs, as they navigate the VUCA environment.

1.8. Scope of Research/Delimitation of the Study

There are limited studies on risk management, let alone cyber risk management in SMEs. Most studies have tended to focus on risk management in financial services organisations. While risk management is a broad subject, this study focused on cyber risk management with respect to governance, assessment, risk reduction practises, risk transfer and risk awareness and training and impact on performance and sustainability of SMEs domiciled in the city of Harare, Zimbabwe. The study focused on cyber risk management practices of SMEs in-order to understand the level of maturity of the risk management practices and its impact on their performance. Further, the study targeted senior executives in these entities (i.e. chief executive officers, risk managers and finance executives) as they were expected to provide risk leadership in their companies. The study also utilised current data covering a period of 2015-2019, as this period brought about a number of cyber related operational issues due to the volatile environment in which the SMEs operate in.

1.9. Dissertation Outline

The study was organised under the following chapters:

Chapter One

This chapter provides an introduction into the research area and a detailed background on the Cyber Risk Management issues faced SMEs. Further details are provided on the research problem, research aims and objectives, research questions and hypothesis that will be tested. The chapter contains the rationale together with the scope of the study.

Chapter Two

Chapter Two presents a critical review of related literature on Operational Risk Management and more specifically Cyber Risk models, frameworks and performance in the context of SMEs. Further, the chapter outlines a review of key empirical studies into the study area and concludes with the identification of research gap and the conceptual framework underpinning this study.

Chapter Three

Chapter Three outlines the research process and strategy adopted to collect the data required to answer the research questions outlined in chapter one. This chapter explains the research philosophy, design, approach, strategy and implementation of data collection methods. Details of the target population, sampling approach and ethical issues are also included in this chapter.

Chapter Four

Chapter Four presents the interpretation and analysis of the research findings to answer to the research questions. The chapter tests the research hypothesis and develops a regression model for Cyber Risk Management of SMEs. The findings from the primary data analysis are compared with literature review in order to provide an in-depth interpretation and implication of the research.

Chapter Five

Chapter Five concludes the research by summarising the research findings in light of the aims and objectives of the study. The chapter also highlights conclusions drawn from the research and proffers practical recommendations to the government, SME owners and policy makers concerning Risk Management in the sector.

1.10. Chapter Summary

The aim of study was to assess the state of Cyber Risk Management and its impact on SME performance in context of Zimbabwe. This chapter provided the background of the Cyber Risk Management challenges affecting SMEs in Zimbabwe. It also covered statement of the problem, research objectives, questions, hypothesis and rationale of the study. In this chapter, scope and limitations of the study, and dissertation outlines were also presented. The next chapter will cover critical review of related literature to Cyber Risk Management in general and of SMEs in particular.

Chapter 2: Literature Review

2.1 Introduction

This chapter contains a critical review of literature on the impact of Operational Risk Management, particularly Cyber Risk, on the performance of SMEs. The chapter starts by defining the key terms used in the study, cyber risk and risk management, followed by an outline of the key models and theoretical frameworks in the field of risk management. The literature further presents an empirical review of studies which have investigated the relationship between Risk Management and business performance and further presents emerging themes in the field of cyber risk management for SMEs. A conceptual framework adopted for this study will conclude the chapter.

2.2 Definition of Key Terms

2.2.1 What is Risk

The term risk is frequently used in every day operations of business, yet there is no consensus on what the term really means (Kopia, 2017). Several authors view risk as any negative event which results in business losses (Kopia *et al.*, 2017), while others define it as the effect of uncertainty which results in negative or positive outcomes (COSO, 2017; ISO, 2018; Teoh *et al.*, 2017). The insurance industry has historically pioneered the development of downside view of risk, associated with loss and negative effects.

In more recent years, the view towards risk has evolved. There is now a growing convergence towards widely accepted definition of risk as the impact or effect of uncertainty on achievement of an enterprise's objectives (Berg, 2010; ISO, 2018; Teoh *et al*, 2017). The modern definition provides two distinct views on risk i.e. as either negative, in which case it has to be managed, and as a positive, in which case it has to be exploited. According to Berg (2010), risk is *"the uncertainty that surrounds future events and outcomes which is expressed in terms of likelihood and impact of an event with the potential influence the achievement of organization objectives."* This definition is consistent with the definition provided by ISO 31000: 2004, 2009 and 2018, which defines risk as the effect of uncertainty on objectives.

While a variety of definitions of risk were presented above, this research defines risk as any future event with the potential to bring disruptions to the attainment of an organisation's objectives.

2.2.2 Small and Medium Enterprise

a) SMEs: Global context

According to Nyathi et al. (2018), the definitions of SMEs vary across industries and from country to country. As such, there is no globally agreed definition of an SME, even in one country (Helmsing, 1993; WBCSD, 2007). It was noted that SMEs have various definitions depending on the industry in which they operate. (Helmsing, 1993). Nyathi et al. (2018) highlights that it is difficult to capture all the characteristics of SMEs or to detail the differences between SMEs in different sectors or countries. Furthermore, Natarajan and Wyrick (2011) notes that the definition, conceptualisation and composition of what an SME is in different countries is a fluid concept, and still attracts a variety of ideas. Different authors have varying definitions of SMEs, depending on the target group (Abor and Quartey, 2010). Amongst others, the key factors or bases in most definitions of SMEs are based on:

a) the number of employees,
b) capital base of the firm,
c) market share,
d) sales turnover, and
e) the infrastructure of the firm.

However, according to Macpherson and Holt (2007), none of the above constructs are at the same level across industries and national boundaries. Definitions of the size of enterprises, as argued by Weston and Copeland (1998), suffer from global application because they are conceived in different contexts.

According to the European Commission (2003: 39), "SMEs are defined as the category of micro, small and medium-sized enterprises (SMEs) that is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." The table overleaf highlights a summary of measures used by other international organisations with offices in Zimbabwe:

Table 2.1: SME definitions used by Multilateral Institutions (with sub – offices in Zimbabwe)

Institution	Maximum Number of Employees	Maximum Revenue or Turnover (US$)	Maximum Assets (US$)
World Bank	300	15,000,000	15,000,000
African Development	50	None	None
UNDP	200	None	None
EU	250	50,000,000	43,000,000

Source: Brooking Global Economy and Development (2008)

A different definition is provided by the Zimbabwe Revenue Authority (ZIMRA), which defines SMEs in terms of points scored on employment, turnover, and total assets value as shown below:

Table 2.2: ZIMRA definition of SMEs

Base	Range	Points	Factor
Employment	up to 5 employees	1	A
	6-40 employees	2	
	42-75 employees	3	
	76 and above employees	4	
Turnover (Annual)	up to US$50,000	1	B
	US$50,001 to $500,000	2	
	US$500,001 to $1,000,000	3	
	$1,000,001 and above	4	
Gross asset values	up to US$50,000	1	C
	US$50,001 to $1,000,000	2	
	US$1,000,001 to $2,000,000	3	
	$2,000,001 and above	4	

Source: ZIMRA data (2016)

Based on the ZIMRA table above, any corporate which scores combined total points below 7 points in all the three bases (i.e. Employment, Turnover and Gross Asset Value), falls within the SMEs category.

A different definition of SMEs is given by the Ministry of Small and Medium Enterprises (MoSME). According to MoSME (2015), a small enterprise in Zimbabwe is a company which employs not more than 50 employees whilst a medium enterprise employs between 75 to 100 employees. It is important to note that this definition is different across sectors in Zimbabwe as shown overleaf:

Table 2.1: MoSME Definition of SMEs

Industry	Size	Number of Employees
Manufacturing	Small	50
	Medium	100
Mining	Small	50
	Medium	100
Agriculture	Small	50
	Medium	100
Transport	Small	30
	Medium	50
Construction	Small	40
	Medium	75
Wholesale	Small	50
	Medium	75

Source: Ministry of Small and Medium Enterprises and CD Policy Document (2009)

Another definition is given by the Small Enterprises and Development Cooperation (SEDCO) (2010) which refers to SMEs as entities which employ less than 100 personnel, with a revenue up to a maximum of US$830 000. The definition by SEDCO, however, does not clearly distinguish any difference between small and medium entities. For the purposes of this study, the researcher adopted the definition by ZIMRA in the table 2.2 above.

2.2.3 Defining Cyber Risk

Table 2.3 below provides synopsis of different definitions of cyber risk:

Table 2.2: Definitions of cyber risk

Author	Definition
Bohme and Kataria (2006)	Failure of information systems due to worms and viruses.
National Association of Insurance Commissioners (Working Papers On Risk Management And Insurance, No. 151 – January 2015)	A multitude of different sources of risk affecting the information and technology assets of a firm. Examples include identity theft, disclosure of sensitive information, and business interruption
Institute of Risk Management, Cyber Risk Executive Summary Report (2014)	Any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.
RSA Whitepaper, Cyber Risk Appetite (2016)	Cyber risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems. More broadly, “the potential of loss or harm related to technical infrastructure or the use of technology within an organization.

Author	Definition
Chief Risk Officers (CRO Forum, 2014)	Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks
Geneva Association (2016)	Any risk emerging from the use of information and communication technology that compromises the confidentiality, availability, or integrity of data or services."
(Mukhopadhyay et al. 2013)	Business disruption or financial loss caused by malicious electronic intent
Swiss Re (2014)	“Any risk emanating from the use of electronic data and their transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud commit by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information.”
ISO 27 0000 series	The potential occurrence of events or incidents that might materially harm the organization’s interests
COBIT	The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
Cebula and Young (2010)	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems.
PWC	“Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data”

Source: Own compilation (2019)

While the internet might be the main source of cyber threats (due to its public domain), cyberspace describes every network that connects IT systems (e.g. LAN, WAN). Several other definitions emphasize the significance of networks (Swiss Re, 2014; CRO Forum, 2014). In comparison, other authors do not stress the term “network” explicitly as constitutive and use broader definitions. For example, Cebula and Young (2010) define cyber risks as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems”.

Similarly, the National Association of Insurance Commissioners (2013) list identity theft, disclosure of sensitive information and business interruption as examples of cyber risk. Other researchers investigate only one particular type of cyber risk, such as data breaches (Böhme and Kataria, 2006). Others see the motivation of the attacker as relevant. For instance, Mukhopadhyay et al. (2005, 2013) concentrate only on malicious events.

2.2.3.1 Other key definitions related to cyber risk

a) ***Cyber Security*** *- Cybersecurity is the process of protecting information by preventing, detecting and responding to attacks (NIST).*

b) ***Cyber event, cybercrime and cyberattack*** *- These terms are at times used interchangeably. They have been defined in many ways, and yet no widely agreed upon way of differentiating between. According to Hathaway and Croofof (2012), different views on cyberattack and cybercrime are based on the actors involved, means, or the objectives of the risk event. Therefore, cyberattack is defined as "any action taken to undermine the functions of a computer network for a political or national security purpose" (ibid). A more common definition of cybercrime is "any crime that is facilitated or committed using a computer, network, or hardware device." It should therefore be noted that cyber event is a broader term that encompasses the aforementioned situations. As such, differentiating between different types of cyber events may not be obvious, if actors and their motives are not readily apparent (Hathaway & Crootof 2012).*

c) ***Malware*** *- Malicious software that is used with the intent to compromise the integrity, confidentiality, and/or availability of data.*

d) ***Distributed Denial of Service (DDoS)*** *– These are attacks which involve flooding the victim with commands to the extent that it becomes inoperable.*

e) ***Brute force attacks*** *– Involves the use repeated attempts to guess a password until the correct one is reached, giving access to some information.*

f) ***Phishing*** *– These are techniques which are used to steal information from users by disguising as a trustful source.*

g) ***Social engineering*** *- techniques that involve human interaction, with an agenda to gain unauthorised access to protected information (Bendovschi 2015).*

2.3 Theoretical Literature review

2.3.1 Conceptual Issues in Cyber Risk

2.3.1.1 Types of Cyber Risk

From the sections above, a narrow definition or view of cyber risk covers exposure to harm and/or loss resulting from breaches of or attacks on information systems. Other definitions presented a broadened view and defined cyber risk as exposure related to technical and/or use of technology by any organisation.

The second view presents multiple ways in which the events which cause cyber risk can be categorised, the first being intent (*RSA Whitepaper, Cyber Risk Appetite, 2016).* Cyber risk events may arise due to deliberate acts of malice e.g. hacker carrying out an attack on sensitive information. It can also be unintentional e.g. user error which causes a critical system to be temporarily unavailable. The second consideration is the source of the cyber risk events i.e. inside or outside the business. Outside risk events may be due to cybercriminals or supply chain partners, and sources inside the company include employees and/or contractors (ibid).

Further to the above, the Basel III operational risk framework classifies cyber risk into four categories. These include (1) actions of people, (2) systems and technology failure, (2) failed internal processes, and (4) external events (Biener, Eling, and Wirfs; 2015). Presented in the table below are the risk components and description of the risk source:

Table 2.3: Categorisation of cyber risks

No.	Category	Component	Description of Risk Source
1	**Actions of people**		
	Accidental	Error, mistake	Unintentional actions, no harmful or malicious intent
	Intentional	Vandalism, theft, fraud, sabotage	Deliberate action with harmful intent
	Inaction	Insufficient skills, personnel, knowledge	Failing to act or take action in a situation
2	**System & technology failure**		
	Systems	Integration, complexity, specs, design	Systems fail to perform as expected
	Hardware	Lacking capacity, maintenance, performance	Failure of physical equipment
	Software	Security, testing, compatibility, configurations	Failure of software
3	**Failed internal processes**		
	Process controls	Review, monitoring, process ownership	Process operations with inadequate controls

No.	Category	Component	Description of Risk Source
	Process execution/design	Process & information flow, documentation, alerts, agreements	Poor execution/design leading to process failure
	Process support	Staff, accounting, training, development	Supporting process fails to deliver resource
4	**External events**		
	Business	Economy, market, supplier	Business environment change
	Catastrophes	Unrest, weather, fire, flood	Events, without notice, which cannot be controlled
	Legal	Litigation, compliance, legislation	Legal risks
	Service dependence	Transportation, utilities emergency services	Dependence on external parties

Source: (Biener et al. 2015; Cebula & Young 2010)

The above categorises dovetail into the proposals by the Institute of Risk Management in their Cyber Risk Executive Summary Report (2014), who posits that risk manifests in three ways, which include:

- *Deliberate and unauthorised breaches of security to gain access to information systems for the purposes of espionage, extortion or embarrassment.*
- *Unintentional or accidental breaches of security, which nevertheless may still constitute an exposure that needs to be addressed*
- *Operational IT risks due to poor systems integrity or other factors*

Alternative classification of cyber risk is also provided by Kendrick (2010), who proposed three categories i.e. technology risks, legal and compliance risk, and operational risk. Technology risks include risk from presence of the technology itself such as system failures and viruses and are the most obvious of the cyber risks. Another category comprises legal and compliance cyber risks. These are risks which arise from failure to comply with internet technology related regulation. Most of the current statutes and law were formulated with the physical world in mind, and as such, their application to the cyber or online world is not always straightforward (ibid). The last category is operational cyber risk, which arise from use of computers and networks in their business operations and practices e.g. the use of email.

A key important aspect to note from all the categorisation presented above is that there is no ready clear-cut demarcation between these proposed categories. As such there can be overlapping cases and the classes are not mutually exclusive.

2.3.1.2 Cyber Risk Management and Enterprise Risk Management Approach

One important aspect of sound risk management is that cyber risk is not the responsibility of the IT department; it requires an overarching dialog between different departments (e.g. sensitization, trainings). Moreover, the institutional commitment – demonstrated by having a person responsible for information security – is very essential. Firms with a Chief Information Security Officer or a similar position have lower average costs when a breach occurs (US$157 per record vs US$236 per record for firms without strategic security leadership; Shackelford, 2012).

The first step in the classical risk management process is to define the initial situation and goals of the cyber risk management. There exist a multitude of industry standards, in particular from the field of IT, which can serve as templates for cyber risk management. Some of these standards are discussed in the sections below.

2.3.1.3 Global Cyber Risk Management Frameworks

To guide organisations in the management of cyber risk, several frameworks were developed over the years. While a number of corporates across the globe agree on the threat posed by cyber risk, and the need to adopt a strategic view on cyber risk management, there are multiple versions of what constitute a cyber risk management process. The most notable frameworks include the National Institute of Standards and Technology (NIST) standards, International Organization for Standardization (ISO/IEC 27001, ISO 31000 and ISO 27005) standards, Committee of Sponsoring Organization of the Treadway Commission (COSO, 2004, 2009 and 2017), and Control Objectives for Information and Related Technology (COBIT).

2.3.1.4 Framework for Improving Critical Infrastructure Cybersecurity

The National Institute of Standards and Technology (NIST)'s Cybersecurity Framework reflects one of the most comprehensive frameworks on the breadth of cybersecurity. The Cybersecurity Framework lists 5 core functional areas for cybersecurity i.e. identify, protect, detect, respond, and recover. From the 5 core areas, 23 categories and 108 subcategories are mapped to various secondary references such as COBIT 5 and the ISO series.

According to Goel et al., (2018), the NIST guidance does not provide a simplified way to implement the framework without deciphering a complex span of technical controls available through references to other standards. Furthermore, some stakeholders have expressed an interest in adding a quantitative dimension to the Cybersecurity Framework for accuracy of assessment and to reduce subjectivity in its application.

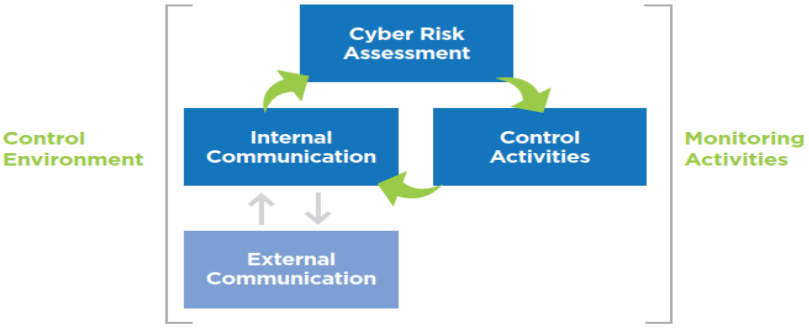
2.3.2 ISO Series

The International Standards Organization (ISO) 27000 standards series includes ISO27001, 27002, 27003, 27004, 27005, and 27006. These standards establish guidelines and general principles to address security issues in order to mitigate risks. They focus on initiating, implementing, maintaining and improving operational, application, computing platform, network and physical security with regard to information within a business. The Information Security Management System (ISMS) is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

2.3.3 A COSO-focused Cyber Risk Assessment

According to COSO, an organization's cyber risk assessment should begin first by understanding what information systems are valuable to the organization (Deloitte, 2012). The value should be measured against the potential impact to the entity's objectives. The 2013 Framework provides several points of focus, within Principle 6, that provides perspective to organizations on how to evaluate its objectives in a manner that could influence the cyber risk assessment process. A summary of the cyber risk assessment process is highlighted in the figure below:

Figure 2.1: Cyber risk assessment process



Source: Deloitte (2012)

2.3.4 COBIT framework

The Control Objectives for Information and Related Technology (COBIT) is a good-practice process-oriented framework for IT management and IT governance, and was created by a professional organization called Information Systems Audit and Control Association (ISACA). It assists businesses in aligning its IT use with its business goals, as it highlights the business need that is satisfied by each control objective (Ridley et al., 2004). COBIT 5 includes an add-on related to information security and assurance. (Ridley et al., 2004:1). ISACA (2012a) identified the five principles on which COBIT is based as follows:

- *Meeting stakeholder needs to align business and IT goals,*
- *End-to-end coverage of the enterprise that covers all functions and processes, both internal and external,*
- *A single, integrated framework that integrates various other frameworks and can serve as an overarching framework,*
- *A holistic approach that accounts for organizational processes, culture, structures, etc., and*
- *Separate governance and management to de-conflict roles and responsibilities.*

It has been acknowledged that COBIT can deliver much-needed operational rigor, however, implementation has proven problematic. COBIT requires outsourcing help as implementation is typically executed by a third-party IT service provider. In such a scenario, the emphasis is on standardisation and repeatability for the purposes of compliance and certification (Overby, 2012).

The downside is a disconnect with the business processes of the organisation that disincentivizes participation by members of the organisation. It is therefore imperative that cybersecurity be an enterprise-wide approach with complete commitment from the top members of the agency. For the stated purpose of top-down involvement, it is important to have a cybersecurity framework that is easily accessible for executive decision making.

From the analysis above, it is evident that different types of security frameworks are available which SMEs can leverage upon and build their cyber security infrastructure. In reality, no one security framework is enough to build real time security policies because every organisation is different, and it is a fundamental reason why there are no common security frameworks that are set as a standard.

Most authors agree that each organisation should understand the context (internal and external) in which it operates, and set its objectives accordingly. According to Berg (2010), organisations can use SWOT (Strengths, Weaknesses, Opportunities and Threats), and PESTEL (Political, Economic, Societal, Technological, Environmental and Legal) frameworks for environmental scanning.

With a context of the environment and set objectives, the next step is for the manager to determine the cyber risks that are likely to affect the organisation. To assist in the risk identification process, organisations can employ a number of tools and techniques that include structured interviews, expert interviews, brainstorming, checklists and focus group discussions (Kopia et al., 2017).

2.3.5 Theories Underpinning Risk Management

This section reviews the literature on the financial economic theory, the agency theory, modern portfolio theory and complexity theory in the context of Risk Management and corporate performance.

2.3.5.1 Agency Theory and Risk Management

The agency theory posits that risk management is necessary to mitigate the different interests of agents and principals in an organisation. (Smith and Stulz, 1985). According to Mayers and Smith (2019), the divorce of ownership and control in organisations and the asymmetric distribution of information and earnings, creates motivation for the agent to engage in excessive risk-taking behaviour. The Agency theory focuses on financial risk management through hedging. It is important to note that due to the limited scope of the agency theory, only few empirical studies were carried out to validate the theory, some of which have failed to validate the theory (Faff and Nguyen, 2002; Geczy et al., 1997).

In some SMEs, Managing Directors are appointed to run the organisation on behalf of the owners, hence there is inherent agency conflict. Furthermore, the SMEs employ more agents in the form of finance managers, marketing managers and/or production managers who all have self-interest that create conflict in the organisation.

2.3.5.2 Financial Economic Theory of Corporate Risk Management

According to Modigliani and Miller (1963), under conditions of perfect capital markets, the financial structure of firm does not have any bearing on the market value of firm. As such, there is no value in carrying out any risk management initiatives, since the "perfect capital markets" will be able to price risk fairly (Grace et al., 2010). When the assumption of perfect markets is relaxed, there is consensus that risk management can create firm value by reducing and/or exploiting market imperfections caused by taxes (Modigliani, 1963), bankruptcy costs (Smith and Stulz, 1985), information asymmetry (Geczy et al., 1997), and agency costs (Jensen and Meckling, 1976). It is important to note that empirical evidence to support risk management implications on financial economic theory have been mixed (Carter et al, 2006; Jin and Jorion, 2006).

The relationship between cyber risk management and value creation, arises from the belief that risk management minimises the likelihood of financial distress. This enables an organisation to borrow funds, and benefit from tax benefits associated with interest payment. SMEs operate in an environment which is not only imperfect but also volatile, uncertain, complex and ambiguous. As such, those SMEs who can anticipate these market imperfections in advance, and implement sound risk measures, will be able to achieve sustainability.

2.3.5.3 Markowitz's Portfolio Theory (MPT) and Risk Management

Markowitz (1952)'s mean-variance model, also referred to as the Portfolio Theory, gave rise to risk management using an integrated approach (CAS, 2003; Alexander, 2009). According to MPT, securities should be selected based on their return and standard deviation (risk). Further to this, consideration should also be given to their correlation (preferable negative correlation) with other securities.

The new approach to risk management i.e. Enterprise Risk Management (ERM), borrows heavily from MPT in its approach to cyber risk management. In supporting the modern approach to risk management, CAS (2003) highlights that managing cyber risks in silo is inefficient and counter-productive, as some identified risk often provide "natural" hedges to others. Further to this, the Committee of Sponsoring Organisation (COSO) Integrated Framework (2017), provides for a "portfolio view of risk" as one of the principles under the performance component. More recently, the International Standards Organisation (ISO) 31000:

2018, highlights that risk analysis must consider complexity and connectivity of factors, a concept which underpins the portfolio view to risk. In summary, the MPT was instrumental in advocating for an integrated approach to risk, thus enabling organisations to appreciate the interconnectedness of cyber risk within their environments.

2.3.5.4 Complexity Theory and Risk Management

Ross (1940), under the Complexity theory, said that it is not possible to understand and/or describe a system through knowledge of how the individual parts work. As such, a system is an interplay of behaviours, which provides feedback form the other parts produce outcomes which cannot be predicted by knowing the individual constituent of that system.

To address the above complexity, COSO updated its risk management framework in 2017. The revised framework advocates for an integration between strategy, performance and risk management. According to COSO, the future of cyber risk management lies in leveraging advanced analytics, automation, artificial intelligence and data visualisation to clearly understand the evolving risks and to uncover unrecognisable relationships and patterns.

The complexity theory is important to the research as it unpacks the VUCA operating environment and the interrelatedness of the risk it brings. It further assists business owners and managers to develop and adopt more sophisticated cyber risk management approaches beyond the simple traditional assessment which were carried out over the past years.

2.3.5.5 Classical Decision Theory

The classical decision theory states that risk is perceived as reflecting variations in the distribution of likely outcomes and their subjective values. Hence a risk alternative is one where the variance is large, and risk forms an important factor in evaluating alternative options. Decisions are said to be taken under risk when there is a possibility of more than one outcome resulting from the selection of an option. Furthermore, it is assumed that the probability of occurrence of each is known to the decision maker in advance. The variation in outcomes is said to be consequence of factors which are beyond his control (Radford, 1978)

Decision Theory is implicitly contained by the cyber risk management process, since risk management depends on rules derived from general knowledge and precepts of Decision

Theory (Vaughan, 1997). Once a risk has been past the assessment phase, a decision must be made regarding what –if anything– should be done, thus different approaches to risk management decisions are possible.

2.3.5.6 Theoretical Benefits of Cyber Risk Management

Traditional scholars advocate for cyber risk management on the back of the financial economics theory, which posit that effective risk management activities reduce costs related to imperfect capital markets i.e. information asymmetry, tax, bankruptcy and agency costs (Kraus and Litzenberger, 1973; Nocco and Stulz, 2006; Smith and Stulz, 1996). Furthermore, it reduces the impact of costly lower tail outcomes and likelihood of financial distress, thus creating value for the company (Stulz,1996).

The growing and dynamic trends in cyber risk have caught the attention of researchers who seek to investigate its impact on business performance. Key research title was to investigate the impact of cyber risk on SME performance. These empirical studies are the subject of discussion in sections 2.4 and 2.5.

2.3.5.7 Business Performance Dimensions

Performance measurement is pivotal in assessing the impact of business initiatives. However, the matrices for measuring such vary from author to author. With regards to general performance management, financial proxies such as return of assets, sales growth, return of equity are used (Baxter et al., 2013; Ramlee and Ahmad, 2015).

2.4 Empirical Literature Review - Cyber Risk Globally, in African and the Zimbabwean Context

2.4.1 Cyber Risk Globally

Cyber risk was ranked 1st in more than 40% of OECD countries (Global Risk Report, 2017). By 2021, the global cost of cybersecurity breaches is expected to reach US$6 trillion, double the total for 2015 (Global Crime Report, 2017). The World Economic Forum's report on Global Risk (2017) now rates a large-scale breach of cybersecurity as one of the five most serious risks facing the world today. To address the growing phenomenon of cybercrime and data lost, countries such as India (Joshi *et al.*, 2005), Malaysia (Fatt and Wahjanto, 2005), Singapore

(Chia, 2005) and the United Kingdom (Griffiths and Harrison, 2005) have developed laws to deal with cyber risk.

These countries have also developed strategies that stimulate the advancement of information security (Salzberg and Jang, 2012). Such strategies include development of laws such as the Electronic Communication Law of 2005 in the Czech Republic (Szeman, 2005), the Information Technology Act of 2000 in India (Joshi *et al.*, 2005), the Electronic Transactions Act of 1996 in Singapore (Chia, 2005), and the Malaysia Digital Signature Act of 1997 in Malaysia (Fatt and Wahjanto, 2005).

2.4.1.1 Costs and detrimental effect caused by cyber risk

Anderson et al. (2013) argue that most cyber costs are indirect losses (e.g. loss of trust), and defence costs (e.g. antivirus software and insurance), excluding direct losses (e.g. theft of money). To evaluate both direct and indirect effects, several studies were done to investigate the impact which cyber risk incidences have on companies' stock prices. Cavusoglu et al. (2004) showed that a security breach negatively affects a company's stock price. Estimated loss was up to 2.1% of the market volume. A major part of the discount is explained by the reputational damage (Sinanaj and Muntermann, 2013). However, Campbell et al. (2003) showed that a breach of confidential data has a larger negative effect on the stock price, than non-classified information. Furthermore, Hovav and D'Arcy (2003) showed a negative price effect for companies with a business model that is heavily based on the internet.

2.4.2 Cyber Risk in Africa

In most developing nations such as Zimbabwe, there has been a paradox where the increased access to internet and other technologies has had the effect of increasing the rate of malware and exposure to cyber threats. This is because such countries are less mature in their security capabilities (Nicholas, 2014).

Developing countries such as Zambia and Zimbabwe suffer from cybercrimes amounting to 0.14% and 0.16% of GDP respectively (McAfee Intel Security, 2014). On the continent, there is the African Union Convention on Cybersecurity and the Personal Data Protection (2014), which seeks to harmonize African cyber legislations on e-commerce, corporate entities, personal data protection, cyber security promotion and cyber risk control (Nyirenda-Jere & Biru, 2015).

2.4.3 Zimbabwean Context

Despite the growing global concern towards cyber risk, Zimbabwe has no cyber security framework (Ministry of Information and Communication Technology, 2015). New legislation is currently being drafted, which will cover e-commerce, cybercrime and data protection. This Bill attracted a lot of attention because it addresses how citizens use technology everyday through services like social media and sharing Wi-Fi connections. (Gambanga, 2016).

According to the Reserve Bank of Zimbabwe (RBZ, 2015), cybercrime accounts for an estimated US$1,8 billion in illicit annual proceeds generated from criminal activity in Zimbabwe. Between 2011 and 2015, about 140 cybercrime cases were reported, and these include; Phishing (20); Credit Card Fraud (13); Identity Theft (10); Unauthorised Access (24); Hacking (72); and Telecommunications Piracy (1) (ibid). Further, approximately 37 government related sites were hacked between 2013 and 2016 (MISA-Zimbabwe and Digital Society Zimbabwe, 2016).

These Zimbabwean statistics above are evidence of the vulnerability faced by SMEs to computer and cyber risk, hence the need improve cyber risk management in these organisations. Further empirical evidence is provided in the section below.

2.5 Theories on SMEs and Risk Management

2.5.1 An empirical review of cyber risk for small and medium-sized enterprises

An area of concern for SMEs centres on encouraging good security behaviour by employees (Taylor and Murphy, 2004; Nurse et al., 2011). Through development of a strong security culture, many behavioural issues can be addressed which underpin data breaches in SMEs (Santos-Olmo et al., 2016; Contos, 2015; ENISA, 2019). As such, the development of cybersecurity skills involves addressing digital threats using technology and complementary factors such as policy guidelines, organisational processes and cyber risk awareness strategies. According to Dojkovski et al., (2017) SMEs can improve overall security through an organisational security setting where employees naturally protect corporate information assets.

Some SMEs can be a difficult audience, particularly those who may not comprehend the importance of cyber risk management or whose owners and key influencers are completely immersed in the day-to-day operations of the business (OAS, 2015). According to Bada et al., (2015), a manager or owner's knowledge, and understanding of cyber risk, as well as their experiences influences behaviour. A gap which remains is how to best encourage good cyber risk management behaviour. Such behaviour needs to be dynamic and continue into the future, hence mitigating the variations in cyber risk from period to period (Nurse, 2018; Iuga et al., 2016). This has led to SMEs shunning cyber risk management, or for those that do, a general lack of certainty on how best to respond to cyber risk while still avoiding cyber risk fatigue and technicalities brought by the always changing nature of the risk. (Furnell and Thomson, 2009; InfoSecurity, 2017).

In the US, research was carried out on the challenges SMEs face in cyber risk management. Specific recommendations were made regarding educational, software and hardware tools (Asti, 2017). The Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018) also emphasises this point. This means that all employees (including executives) along with third-party stakeholders are to be trained. A campaign, "Stop Think.Connect" (US DHS, 2018), provides cyber risk management tips for larger corporate and SMEs.

In developing countries such as Zimbabwe, the requirement to strengthen cyber risk management for both large corporates and SMEs has been acknowledged (Kabanda et al., 2018). For SMEs, cyber risk management is hampered by internal factors of such as budget, managerial support and attitudes (Kabanda et al., 2018). In Uganda, research is aimed at better positioning SMEs to administer cyber risk management, thus equipping them with key skills pertaining to both online and offline cyber risk awareness activities (CIPESA, 2017).

The quest to strengthen cyber risk management affects both SMEs and large corporates. From an academic perspective, the starting point is for managers to identify key assets and understanding the pertinent cyber risks (Agrafiotis et al., 2018; and Valli et al., 2014). Such actions will enable managers to design effective cyber risk management plans to protect the business and foster employee engagement. In literature, these can be thought of as asset/harm-based approaches to cyber risk management, hence protecting the critical assets of the business. It should be noted that cyber risk management by SMEs should be holistic, at the same time appreciating the limited resources at their disposal.

The literature review above has provided guidance on many of the important aspects of cybersecurity as it relates to SMEs i.e. culture, security-orientation and SME engagement. These approaches rely on proactive involvement by the SMEs. However, operating in a VUCA environment, SMEs are more concerned about daily operations and survival. As such they are less likely to know about and/or proactively adopt leading cyber risk management practice (OAS, 2015). The literature analysis above has revealed a gap in research SMEs cyber risk management beyond dissemination of reports and/or standards.

2.5.2 The impact of cyber risk management on corporate performance: an Empirical Perspective

A number of researchers have researched the link between risk management and corporate performance. Graham and Rogers (2002) studied risk and firm value, and found a positive association between the two. Furthermore, a positive association was found between the use of ERM and firm performance (Florio and Loeni, 2017; Jenya and Sandada, 2017; Khan and Ali, 2017; Yang and Anwar, 2018).

The table below summarises some of the studies on risk management and corporate performance:

Table 2.4: Empirical studies on risk management and performance

Author(s)	**Methodology Used**	**Result Summary**
Gates *et al*. (2012)	Survey	Use of ERM increased management consensus, better-informed decisions, enhanced communication and greater management accountability
Teoh and Muthuveloo (2015) - impact of ERM on corporate performance in public listed companies in Malaysia	Survey	Positive and significant association between the implementation of corporate performance and firm performance.
Teoh, Lee and Muthuveloo (2017)	Survey	Significant relationship between ERM implementation and firm performance in Malaysia
Jenya and Sandada (2017) - Impact of the 5 main processes of the COSO ERM framework on the performance of SMEs	Survey	Positive and significant relationship between ERM and the performance of SMEs
Yang and Anwar (2018) - impact of ERM among SMEs in Pakistan	Survey	Positive impact of ERM practices on both performance and competitive advantage
Quon (2012) – Impact of risk management on firm performance	Desk research	using ERM variables derived from annual reports of 156 listed financial firms on the Standard and Poor Composite index, no evidence was found to support that ERM improves business performance during the period 2007 and 2008.

Author(s)	Methodology Used	Result Summary
Alawattegama (2018) - Impact of ERM on the performance of financial services firms, Sri Lanka	Survey	None of the eight key ERM functions as suggested by the COSO ERM integrated framework has a significant impact on firm performance
Norton Report (2013)	Online survey	The consumer was using mobile devices and merging work and personal devices into one. Global direct cost of cybercrime is 113 Billion US dollars.
Kaspersky Global IT Security Risks Survey 2013.	Online interviews	IT security was the main concern of IT management of an organization; highlighted the use of a personal mobile device at work, and data leakage through insiders.
CERT US State of Cybercrime Survey (2013)	Online survey	The results reflected the effect of insider attacks on organizations. Results concluded that insider attack was worse than outside attack.
Cost of Cyber Crime Study: 2013 Global Report.	Telephone interview	Highlighted the cybercrime situation in Canadian business operation. Finding included different cybercrime threats victimization and their approaches to tackle them.
Ambrož Milan (2012) Security Culture Impact on Security Excellence in a Company	Hands on Interview	The impact of security culture characteristics, on the behaviour of employee regarding security.
Kaur, J.; Mustafa, N., (2013) "Examining the effects of knowledge, attitude and behaviour on information security awareness."	Interview	Information security awareness among employees without technical background.

Source: Author's compilations

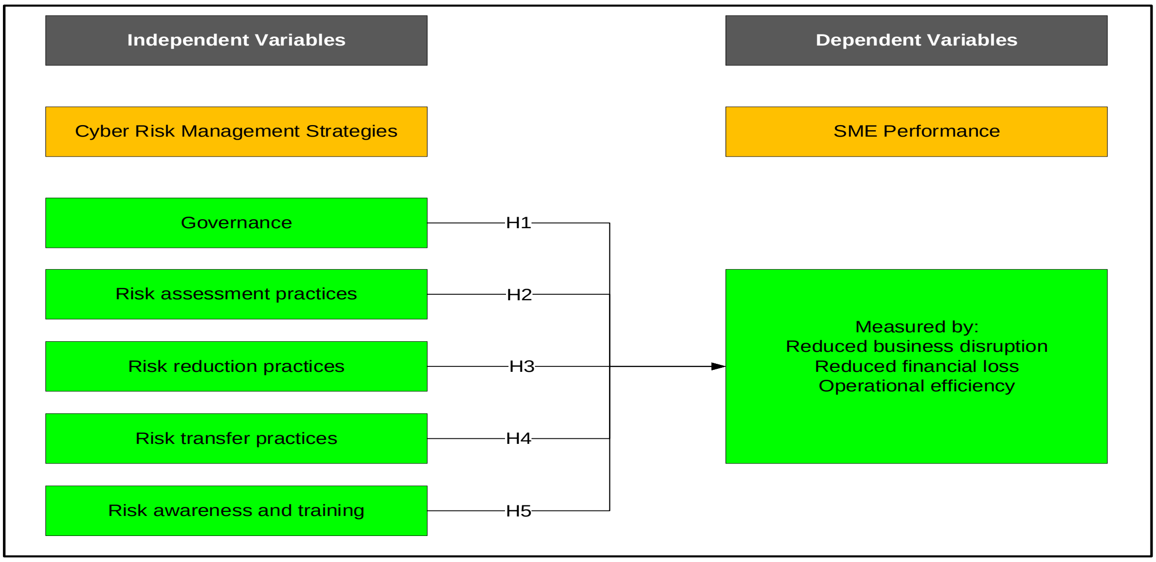
Based on the results above, implementing a cyber risk management programme is a complex process which requires investments in both technology and human capital (McShaine et al., 2011). Due to the varied results presented above, this study seeks to provide new empirical evidence on a dynamic area of cyber risk management in a developing country like Zimbabwe. This area has not attracted much attention and as such will add to the body of knowledge.

2.6 Conceptual Framework

2.6.1 Key Variables and Conceptual Framework

The conceptual framework adopted for this study is based on the OECD measurement framework for digital security risk management in business. This framework represents a consensus amongst OECD countries on the constituents of desirable practices with regard to digital security risk management (OECD, 2011).

The OECD (2019) framework highlights that cyber risk management should address governance, risk assessment practises, risk reduction practises, risk transfer and risk awareness and training. The same dimensions are also mentioned as necessary in other frameworks such as the ISO 27001 and COSO cyber risk frameworks. The OCED framework is yet to be tested empirically in developing countries such as Zimbabwe, and therefore presents an opportunity to develop a deeper and more practical perspective of this framework. As such, this study will adapt this framework to suit the SMEs in Zimbabwe.



Source: Author's compilation

Presented above is the conceptual framework which links five dimensions of cyber risk management to the achievement of an SMEs performance objectives. The five dimensions are hypothesized to positively impact on the attainment of SME's performance objectives.

2.7 Chapter Summary

This chapter was focused on reviewing literature on cyber risk management. In this chapter, a presentation was made on the holistic definitions of cyber risk management and the different cyber threats faced by organisations in their operations. This chapter also introduced the different theories applied to risk management and in particular cyber risk, in an effort to better understand the phenomenon. Furthermore, a discussion was made of the different types of cyber risk and their categorisation; the different frameworks developed to manage cyber risk; how cyber risk has evolved across the globe, in Africa and in Zimbabwe. Lastly, the chapter presented the adapted conceptual framework for this study.

Chapter 3: Research Methodology

3.1 Introduction

This Chapter focuses on the research methodology used in this study. It describes the research design and the rationale behind the design choice. A presentation of the research philosophy and the research paradigm are made, and a discussion on the ethical issues which influenced the study. The chapter further presents a description of the research method, approach and strategy. Various statistical methods employed by the researcher to ensure validity and reliability of the instruments are also discussed in detail. The chapter concludes with a discussion on data Analysis and presentation.

3.2 Research Design

The aim of the study was to investigate the impact of Operational Risk Management, particularly Cyber Risk, on the performance of SMEs. As such, the researcher engaged an explanatory research design to measure and establish the strength of the relationship between the cyber risk management and performance of SMEs. SME performance in this case was measured by reduced business disruption, reduced financial losses, and increased operational efficiency. In addition, the study has clearly defined independent variables, as presented in the conceptual framework. The researcher sought to test five hypotheses about the relationship between these variable and SME performance in Zimbabwe.

3.3 Research Philosophies

3.3.1 Ontological Belief

The study followed an ontological belief as it needed to generalise the research findings to all SMEs through summary measures and statistical analysis. The researcher believes that despite the complications brought on by the VUCA environment to the envisaged relationship, it is possible to measure the impact of cyber risk management on the performance of SMEs and generalise and apply the findings across SMEs operating in similar environments. In short, the study adopted the belief of “one truth” by taking an objective view of reality.

3.3.2 Epistemological Belief

To establish the *"one truth"* mentioned above, the researcher anchored the study on facts gathered through a disciplined scientific research approach. To this end, the research instrument had closed ended structured questions which required no personal opinion or perception of the researcher. Furthermore, the instrument was made to be compatible for statistical manipulation, thus allowing hypothesis testing.

3.3.3 Axiological belief

The research believes that research ethics are an important element of the study and therefore adhered to the following ethical considerations:

- *Informed consent was obtained from the respondents;*
- *Anonymity of the respondents, as well as confidentiality of information collected was maintained;*
- *Exercising restraint in forming biased opinions while carrying out the study; and*
- *Capturing data from respondents in its natural form, without making amendments to any of the information collected.*

3.4 Research Paradigm

The researcher took a positivist paradigm as it allowed the study to objectively quantify the relationship independent of the researcher. The choice of positivism is in line with the research by Antwi and Hamza (2015) that explains how positivism is about adopting scientific methods and quantification to augment the precision in describing parameters and the existing relationship among them. With the support of literature, the study begins with the theory that cyber risk management positively influence the performance of SMEs.

3.5 Research Approach

A deductive research approach was adopted in line with the explanatory research design and positivism research paradigm. The research approach followed theory on the positive relationship between cyber risk management and SME performance, with the view to generalise it to other SMEs. The deductive research approach was also used because the variables of the study were already known, and that a hypothesised relationship has been established from previous research.

3.6 Research Method

The study used a quantitative research method, through obtaining research evidence from a survey of SMEs on the defined variables. The quantitative approach was most appropriate to quantify and test the impact of cyber risk management on the performance of SMEs. The variables were subjected to statistical manipulation through use of descriptive statistics, analysis of variance (ANOVA) and inferential analysis through hypothesis testing. Furthermore, a quantitative research method was chosen because of its compatibility with the explanatory research design, ontological and epistemological beliefs explained above.

3.7 Research Strategy

Primary data was collected from a representative sample of 256 SMEs through a survey using self-administered structured questionnaires. Due to the large population of SMEs in various economic sectors of the country, the strategy was to stratify the population into 5 keys sectors i.e. Manufacturing, Electricity and Renewable Energy, Wholesale and Trade, Transport and Storage, and Financial Services. Stratified probability random sampling method was then used to draw elements from each strata, due to the variation in cyber risk management across each strata.

The large sample of 256 SMEs was representative enough to generate relevant research evidence which can be generalised. Furthermore, the study targeted senior executives in departments including but not limited to finance, IT, strategy, procurement, and operations who are conversant with the cyber risk management, and therefore required limited or no assistance to complete the self-administered questionnaire. The questionnaire was hand delivered to target individuals to improve response rate. A disclaimer was provided clearly articulating the confidentiality of information shared, names of respondents, and the significance of the study.

3.8 Data Collection Instrument

The data was collected using self-administered questionnaires that were targeted at senior managers in SMEs operating in Harare. The questionnaire, with closed-ended questions, was considered most ideal instrument as it allowed the researcher to collect unbiased data from sample SMEs in a quantitative manner. The questionnaire consisted of three sections (see appendix). Section 1 had general questions that required the respondents to provide their company and background information. Section 2 covered questions aimed at identifying cyber risk management strategies used by the SMEs operating in Harare. Section 3 required respondents to answer questions on the SME performance. A Likert scale was designed for Sections 2 and 3, as it is easy to administer to a large sample size. Thorough the provision of standard responses, it made it easier to score and tabulate and convert the data into quantitative data which is more objective and reliable.

3.9 Instrument Development

The study employed a structured questionnaire covering the five independent variables i.e. governance, risk assessment strategies, risk reduction strategies, risk transfer practises and risk awareness and training, as well as the dependent variable, SME performance. Due to availability of tried and tested research instruments on the impact of cyber risk management on SME performance, the research instrument was adapted from prior studies including OECD (2019), Dojkovski et al., 2005, Mochoge (2013), and Dimopoulos (2014).

3.10 Population and Sampling Design

Zikmund and Babin (2013) define a population as the total group of people from whom the researcher draws a sample for their study. For purposes of this research, the target population was 3216 companies in the SME category registered with the Zimbabwe Revenue Authority (ZIMRA) as at 31 August 2019. The ZIMRA database, rather than MoSME database was used as it provided a more representative population of actively trading and formally registered SMEs operating in the country. Furthermore, tax registered SMEs are easier to contact than unregistered ones whose operations maybe more informal.

3.1.1 Sampling Frame

Saunders et al. (2009) define a sampling frame as a comprehensive list of members of the population from which a sample is drawn. The list of SMEs registered with ZIMRA as at 31 August 2019 formed the sampling frame. The study further defined its sampling unit as a single SME.

3.1.2 Sample Size Determination and Sampling Technique

The study utilised simple probability random sampling method to draw elements from the sampling frame. The researcher chose a random sampling design due to the quantitative nature of the study, thus avoiding bias and enabling the researcher to generalise the findings. Bloomberg, Cooper and Schindler (2008) contend that the sample must be large and bear some proportional relationship with the size of the population from which it is taken and also the level of confidence sought. The Yamane formula was used to calculate the sample size, at a required margin of error of 5%. Using this formula as shown below, the study drew a sample of 256 from the population of 714 registered SMEs as shown below:

n = N / 1 + N (e) 2 = 714/ (1+714*0.05^2) = 256

Where N = population size, e = margin of error = 5%

Therefore, the sample size of 256 from a population of 714 was deemed adequate and representative.

3.11 Credibility

Addressing validity and reliability in any quantitative research is key determinant of the credibility of study findings (Heale and Twycross, 2015). This study conducted validity and reliability tests.

To ensure external validity, 2 cyber risk management consultants, working for a Big 4 consultancy firm, validated the contents of the instrument. Furthermore, a pilot study on 10 respondents was carried out to pre-test the instrument and to ensure suitability and clarity of the research instrument. The respondents who participated in the pilot study were excluded for the main study.

Construct validity is defined as the extent to which a research instrument measures the intended constructs (Heale and Twycross, 2015; Hair et al. 2014). The study employed principal component analysis to test for convergent and discriminant validity the cyber risk management constructs as recommended by Hair *et al.* (2014).

3.11.3 Reliability test

The reliability of the instrument is a measure of how consistently the instrument is able to measures that which it is meant to measure (Tavakol and Dennick 2011). The study utilised the Cronbach's alpha which is the most commonly used measure of internal consistency (Shuttlewowth, 2015). Cronbach's alpha was chosen because it enabled the researcher to assess the internal consistency of the five cyber risk management dimensions and the consistency of the items of the questionnaire in measuring cyber risk management. A minimum value of 0.7 was accepted for good reliability.

3.12 Data Analysis and Presentation

Quantitative Data collected from the survey through questionnaires was edited, coded and tabulated and captured into Statistical Package for Social Sciences (IBM SPSS Statistic *version 25*) and Eviews (10). In addition, the data was analysed through descriptive statistics such as pie charts, graphs and tables to depict the frequencies of the variables. The study also utilised correlation analysis, regression analysis, analysis of variance and hypothesis testing to answer the research questions. In order to quantify and test the relationship between the independent variable and the dependent variable, multiple regression analysis and correlation analysis was were employed by the researcher. The procedures carried out for inferential analysis are detailed below:

3.12.3 Normality Test

The researcher carried out a normality test to establish how the data was distributed. The study adopted the Jarque-Bera normality test procedure to test whether the study variables are normally distributed. It is a necessity to assess normality of the variables since the bivariate correlation analysis, tests of confidence intervals and significance testing, as well as regression modelling requires that the candidate variables be normally distributed. Consequently, it was necessary to conduct the Jarque-Bera normality test to ensure that the normality assumption is met before conducting hypothesis tests, correlation analyses and regression modelling.

The JB normality hypothesis

H0: *The data is normally distributed*

H1: *The data is not normally distributed*

The study employed the p-value approach to determine the normality status of the data. The rejection criterion states that: reject null hypothesis if and only if the probability value corresponding to the Jarque-Bera normality test statistic is less than 0.05. The test was performed at 5% level of significance.

3.12.4 Kolmogorov-Sminorv Test

To ascertain normality for firm size and cyber risk intensity variables, the study employed the Kolmogorov Sminorv test. The conclusions were made based on the asymptotic probability value (Sig.). If this asymptotic probability value is less than 0.05 it implies that the variance is not normally distributed.

3.12.5 Test of independence

To assess whether there is independence of association between firm size and cyber risk intensity, the researcher adopted the independent samples t-test procedure to assess the independence of association between firm size and cyber risk intensity. To analyse this independence of association, the study employed the independent samples t-test with a significance level (α) = 0.05.

3.12.6 Multicollinearity Test

Since the study sought to ascertain the impact of key factors of effective cyber risk management on firm performance, using Ordinary Least Squares, it was therefore critical that the factors be tested for multicollinearity. The correlation coefficients in the Component Correlation Matrix were inspected to check for the existence of significant cross correlations amongst the factors.

3.12.7 Principal Components Analysis (PCA)

Method

Step 1: Get some data: In this step the researcher made use of all the responses from the 207 respondents.

Step 2: Subtract the mean: For PCA to work appropriately, the researcher subtracted the mean from each of the data dimensions. The mean subtracted was the average across each dimension. As such, all the x values have $\bar{x}$ (the mean of the x values of all the data points) subtracted, and all the y values have $\bar{y}$ subtracted from them. This produced a data set whose mean was zero.

Step 3: Calculate the covariance matrix: The researcher then computed the variance – covariance matrix.

Step 4: Calculate the eigenvectors and eigenvalues of the covariance matrix: Since the variance - covariance matrix was square, the researcher computed the eigenvectors and eigenvalues for this matrix. These are rather important, as they contain useful information about the data.

Step 5: Choosing components and forming a feature vector: On this procedure, the notion of data compression and reduced dimensionality was important. Once the eigenvectors were determined from the covariance matrix, they were ordered by eigenvalue i.e. highest to lowest. This gave the researcher the components in order of significance. Components with smaller eigenvalues were ignored, resulting in the final data set having less dimensions than the original.

Step 6: Deriving the new data set: Having chosen the components (eigenvectors) to keep in the data and formed a feature vector, the transpose of the vector was taken and multiplied it on the left of the original data set, transposed.

$$Final\ Data\ =\ Row\ Feature\ Vecture\ \times Row\ Data\ Adjust$$

Where: *Row Feature Vector* - the matrix with the eigenvectors in the columns transposed so that the eigenvectors were in the rows, with the most significant eigenvector at the top,

Row Data Adjust - the mean-adjusted data transposed, i.e. the data items are in each column, with each row holding a separate dimension.

Final Data - the final data set, with data items in columns, and dimensions along rows.

3.12.8 Regression Analysis

The study used regression analysis to model the relationship between the dimensions of cyber risk management as independent variables and SME performance as dependent variable. The estimated regression model based on the conceptual framework is presented below:

$Fp = \alpha + \beta_1 Rg + \beta_2 Ras + \beta_3 Rr + \beta_4 Rat + \mathcal{E}$

The definitions to variables estimated in the model are outlined in table 3.1:

Table 0.1 : Variable labels and definitions

Variable	**Definition**
Fp	Variable measuring the performance objectives of SMEs.
α	Constant
β_i	Measures the partial of change in the performance variable resulting from a unit change in the independent variable *i*
Rg	Independent variable measuring cyber risk governance variables as measured by responses to the questionnaire.
Ras	Independent variable measuring cyber risk assessment variables as measured by responses to the questionnaire.
Rr	Independent variable measuring cyber risk reduction variables as measured by responses to the questionnaire.
Rat	Independent variable measuring cyber risk awareness and training variables as measured by responses to the questionnaire.
$\mathcal{E}$	Measures the effect of all other factors that influence SME's performance other that the independent variables already included in the model.

Source: Author's compilation

The β sign represent the direction of association between each independent variable and the dependent variable. Therefore, a positive β indicates a positive association between the construct and SME performance while a negative β indicates the opposite. Given that the study hypothesizes a positive association between cyber risk management and SME performance, a positive β coefficients for all constructs was estimated. In addition, the model also includes an error term $\mathcal{E}_{I,}$ to cover all other factors that influence SME performance, other that the independent variables already included in the model.

3.13 Chapter Summary

This chapter discussed the research methodology which the researcher employed investigating the impact of cyber risk management on the performance of SMEs. The chapter further presented the proposed research design, together with the guiding ontological, epistemological and axiological beliefs. This was followed by a detailed outline of the research paradigm, research approach, research methodology, and strategy. The chapter also outlined the data collection instrument, and how it was developed. A discussion on population and sampling design presented the target population, the sampling frame, sampling design, sampling element, sampling method and sample size. The procedures for ensuring credibility were then discussed by focusing on strategies earmarked for achieving validity and reliability. The chapter concluded with a presentation of the data analysis methods used in the study.

Chapter 4: Data Analysis, Findings and Discussion

4.0 Introduction

The subsequent sections presents the analysis and interpretation of research findings as well as reconciling the study results to literature discussed in Chapter 2. The data analysis was done with the aid of Eviews (10) and IBM SPSS Statistic (25). The analysis commences by investigating the response rate followed by the reliability analysis and then descriptive statistics where the researcher discusses the demographic composition of the study sample focusing on attributes like educational level, work experience, position in the company, type of industry, number of employees and annual revenue. The sections which follow thereafter include normality test, factor analysis, test of relationship, regression modelling, tests of independence and discussion of results.

4.1 Descriptive statistics

This section of the chapter discusses the research response rate, reliability analysis and the demographic composition of the sample.

4.1.1 Response rate

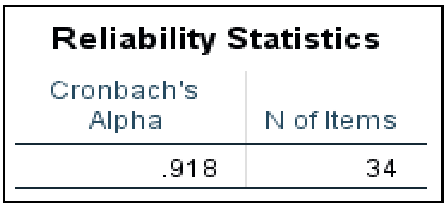
The sample size of 256 from a population of 714 was deemed adequate and representative. Of the 250 questionnaires sent to the SMEs in Harare, 207 were fully marked and returned showing 82.8% response rate. According to Kothari (2008), a response of 70% and above is good for data generalization. This means that the response for this study was excellent and therefore adequate and good enough to ensure the reliability of research findings.

4.1.2 Reliability analysis

The pilot study was conducted to pre-test and ascertain the legitimacy and reliability of the data collection instrument using the 10 questionnaires before the main study. The findings of the pilot study were used to improve some of the questions in the questionnaire. All the vague questions were noted and corrected. Furthermore, an additional role of Cyber Security Manager was added to the questionnaire. These 10 questionnaires were later on included to add to the number of the unit.

The reliability of the questionnaire was knotted using Cronbach's alpha value and the results are as shown in table 4.1. The result provides an analysis of the outcome where the Cronbach's Alpha values were averaged to 0.918 to reflect the scale. This is up-scaled as acceptable according to George and Mallery (2003). It is also closer to 1.0 denoting greater internal consistency of the elements under consideration

Table 4.1: Reliability analysis



Reliability Statistics

Cronbach's Alpha	N of Items
.918	34

Source: Author's compilation from SPSS 25

The average Cronbach's Alpha is 0.918 which can be accepted as excellent within the required Cronbach's alpha coefficient of over 0.7 which gives an assurance of an instrument's consistency and dependability.

4.1.3 Demographic Characteristics

Table 4.2: Demographic composition of the sample

	Frequency	Percent	Cumulative Percent
Level of Education			
O Level	2	1	1
A Level	9	4.3	5.3
Certificate/Diploma	19	9.2	14.5
HND/Degree	61	29.5	44
Post Graduate	116	56	100
Role in the company			
Owner	28	13.5	13.5
Managing Director	35	16.9	30.4
Finance Director	49	23.7	54.1
Information Technology Manager	49	23.7	77.8
Accountant	42	20.3	98.1
Cyber Security Manager	4	1.9	100
Number of employees			
1-20 employees	93	44.9	44.9
21-40 employees	72	34.8	79.7
41-60 employees	29	14	93.7

	Frequency	Percent	Cumulative Percent
61-80 employees	9	4.3	98.1
81-100	2	1	99
Above 100	2	1	100
Annual revenue level			
Less than 1,000,000	15	7.2	7.2
$1,000,001 - $2,000,000	48	23.2	30.4
$2,000,001 - $3,000,000	60	29	59.4
$3,000,001 - $4,000,000	54	26.1	85.5
Above $4,000,001	30	14.5	100
Total	207	100	
Work Experience			
0-1 year	10	4.8	4.8
Greater than 1 year but less than 5 years	51	24.6	29.5
Greater than 5 years but less than 10 years	83	40.1	69.6
Over 10 years	63	30.4	100
Total	**207**	**100**	

Source: Author's compilation from IBM SPSS Statistics version 25

(i) Highest Qualification

It is evident in Table 4.2 that most respondents from the SMEs who participated in the study were holders of Post Graduate degrees (56%); followed by HND/Degree holders (29.5%); Certificate/Diploma holders were 9.2%; A Level, 4.3% and O Level, 1%. The high number of respondents with higher qualifications support the observation that Zimbabwe has a high literacy rate and qualified personnel working in the SMEs. These finding coincides with the results of a study by Odero (2006) who also found that overall level of educational achievement among Zimbabwean entrepreneurs in surveyed firms in Harare is high. Furthermore, De Brun et al. (2009) emphasised that in order to obtain valid results, individuals who have knowledge of the subject must be involved in a study.

(ii) Work Experience

Respondents were asked to indicate the length of time in their management role. The findings show that the majority of the respondents, 40.1% (83) were in their role for more than 5 years but less than 10 years, while 30.4% (63) of the respondents were in their roles for over 10 years. Those with more than 1 year but less than 5 years consists of 24.6% (51). The minority consists of 4.8%, those who had been in their positions for the shortest duration (not more than 1 year). As such, there is reasonable ground to believe that the respondents knew their business operations hence able to provide credible responses to the questionnaire.

(iii) Company's Annual Revenue

Respondents were requested to provide information regarding the annual revenue levels of their SMEs. The information was required to determine the growth of firms. Table 4.2 presents data summary about SMEs' annual revenue levels. As can be viewed in Table 4.2, the majority of the SMEs (29%) reported an annual revenue level of between $2million and $3 million, implying that the a relatively huge proportion of surveyed firms are moderately capital intensive, hence not the typical one man band or backyard informal businesses.

(iv) Number of employees

Findings shown in Figure 4.2 reveal that the majority of the firms were smaller firms with at most 40 employees (79.7%) while 20.3% were medium enterprises.

(v) Role in the company

Findings show that the majority of the respondents constituted the Finance Directors and IT Managers (47.4% combined). Only a meagre, 1.9% consists of Cyber Security Managers. The representation was deemed appropriate for the study purposes as this group's diverse occupations assist in evaluating the impact of cyber risk management on corporate performance. However, the small representation of Cyber Security Managers show that most SMEs do not have dedicated personnel to manage cyber risk within their operations. As such, one person may have multiple roles within the company. Furthermore, it must be noted that the nomenclature obtaining in SMEs has no relationship to performance or affordability of the position by the entity concerned. According to Meijaard et al. (2002), as soon as a small firm hires one or more employees, some kind of organisational structure develops. The actual design of this organisational structure is a mix between intended, deliberate choices and unconscious, emergent developments (ibid).

4.2 Normality test

The researcher carried out a normality test to establish how the data was distributed. The study adopted the Jarque-Bera normality test procedure to test whether the study variables were normally distributed. It is a necessity to assess normality of the variables since the bivariate correlation analysis, tests of confidence intervals and significance testing, as well as regression modelling requires that the candidate variables be normally distributed. Consequently, it was necessary to conduct the Jarque-Bera normality test to ensure that the normality assumption is met before conducting hypothesis tests, correlation analyses and regression modelling.

4.2.1 The JB normality test procedure

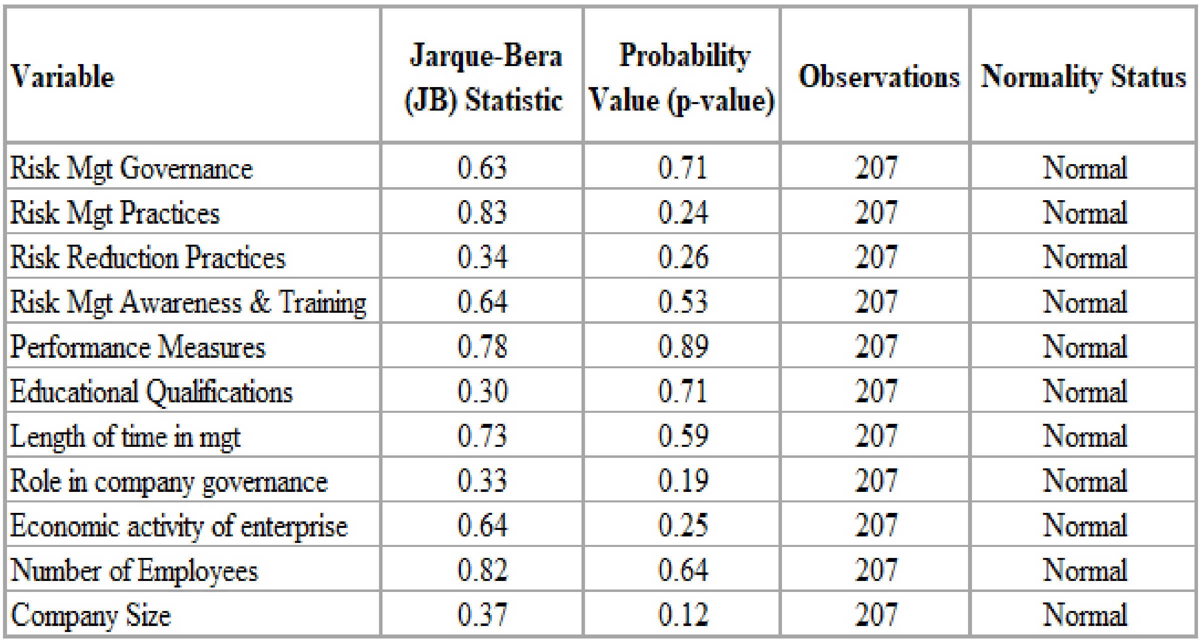
Formulation of hypotheses

H0: The variable is normally distributed

H1: The variable is not normally distributed

The results of the Jarque-Bera normality test are shown in Table 4.3 below:

Table 4.3: Jarque-Bera normality test



Variable	Jarque-Bera (JB) Statistic	Probability Value (p-value)	Observations	Normality Status
Risk Mgt Governance	0.63	0.71	207	Normal
Risk Mgt Practices	0.83	0.24	207	Normal
Risk Reduction Practices	0.34	0.26	207	Normal
Risk Mgt Awareness & Training	0.64	0.53	207	Normal
Performance Measures	0.78	0.89	207	Normal
Educational Qualifications	0.30	0.71	207	Normal
Length of time in mgt	0.73	0.59	207	Normal
Role in company governance	0.33	0.19	207	Normal
Economic activity of enterprise	0.64	0.25	207	Normal
Number of Employees	0.82	0.64	207	Normal
Company Size	0.37	0.12	207	Normal

Source: Author's compilation from Eviews 10

4.2.2 Interpretation of results

The normality test was conducted at the conventional 0.05 level of significance. The results shown in Table 4.3 reveal that all the study variables are normally distributed since all their corresponding probability values are greater than 0.05.

Data for Risk Mgt Governance are normally distributed (p-value = 0.71 > 0.05), Risk Mgt Practices are also normally distributed (p-value = 0.24 > 0.05). Risk Reduction Practices data are also normal (p-value = 0.26 > 0.05), Risk Mgt Awareness & Training, normal (p-value = 0.53 > 0.05). The data for Performance Measures are also normally distributed (p-value = 0.89 > 0.05). All data for the demographic attributes were normally distributed with their probability values being higher than 0.05; Educational Qualifications (0.71), Length of time in company management (0.59), Role in company governance (0.19), Economic activity of enterprise (0.25), Number of Employees (0.64) and Company Size (0.12). Since all the data had been identified to be normally distributed it implies that the results of the correlation analysis, hypothesis testing and regression modelling will be valid since the required normality assumption was met.

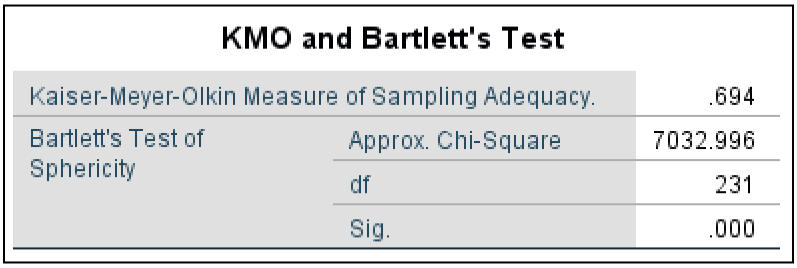
4.3 To investigate the key factors for effective risk management in the context of cyber risk

The second objective of this research was to evaluate the key factors for effective risk management in the context of cyber risk. The section B of the questionnaire outlined the four drivers of effective cyber risk management in SMEs. To attain this objective, the study sought the respondent opinions concerning how SMEs are managing strategic risks. The researcher conducted factor analysis in order to determine the key components for effective cyber risk management in SMEs. The questionnaire had 22 distinct items or questions (also called variables) and each question was ordinally scaled with response categories ranging from 1 through to 5 on a Likert scale. The study employed the principal component analysis to identify key factors of effective cyber risk management.

4.3.1 The Principal Component Analysis (PCA)

The researcher adopted the PCA to determine the critical factors for cyber risk management practices. The questionnaire has 22 questions aimed at ascertaining the effect of cyber risk management practices on performance of SMEs in Zimbabwe. These questions were loaded into SPSS (25) factor analysis to identify questions which load together. Those factors which load together were extracted. To determine whether the data was suitable for principal component analysis (PCA) the study used the Kaiser-Meyer-Olkin measure of sampling adequacy and Bartlett’s Test of Sphericity as shown by the table 4.4:

Table 4.4: KMO and Bartlett’s test



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.694
Bartlett's Test of Sphericity	Approx. Chi-Square	7032.996
	df	231
	Sig.	.000

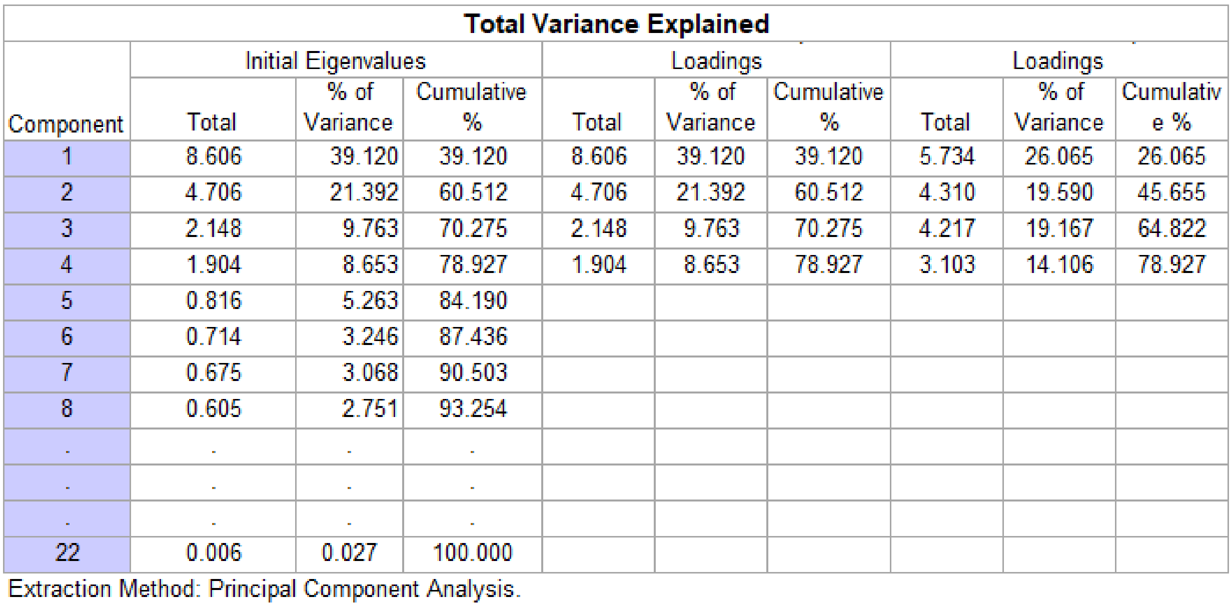
Source: IBM SPSS Statistic version 25

The data is considered suitable for factor analysis if and only if the KMO statistic is greater than or equal to 0.5 and if the probability value of the Bartlett’s test is less than the conventional 0.05 test level. Findings shown in table 4.4 above show that KMO is 0.694 and sig value is 0.000 implying that the data is suitable for factor analysis and it is statistically significant to do so.

4.3.3 Factor Extraction

The factors were extracted from the data based on their Eigen values, where only those factors with Eigen values of at least one were considered important. Factor 1 was named cyber risk governance, Factor 2 cyber risk assessment practices, Factor 3 cyber risk reduction practices and Factor 4 cyber risk awareness & training. Both the total variance explained table and the Scree plot were used to determine the optimal number of factors or constructs to consider for modelling. The results of the factor contribution to effective cyber risk management in SMEs are shown in table 4.5:

Table 4.5: Individual and collective contribution of factors to effective cyber risk management



Total Variance Explained

Component	Initial Eigenvalues			Loadings			Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulativ e %
1	8.606	39.120	39.120	8.606	39.120	39.120	5.734	26.065	26.065
2	4.706	21.392	60.512	4.706	21.392	60.512	4.310	19.590	45.655
3	2.148	9.763	70.275	2.148	9.763	70.275	4.217	19.167	64.822
4	1.904	8.653	78.927	1.904	8.653	78.927	3.103	14.106	78.927
5	0.816	5.263	84.190						
6	0.714	3.246	87.436						
7	0.675	3.068	90.503						
8	0.605	2.751	93.254						
.	.	.	.						
.	.	.	.						
.	.	.	.						
22	0.006	0.027	100.000						

Extraction Method: Principal Component Analysis.

Source: IBM SPSS Statistic version 25

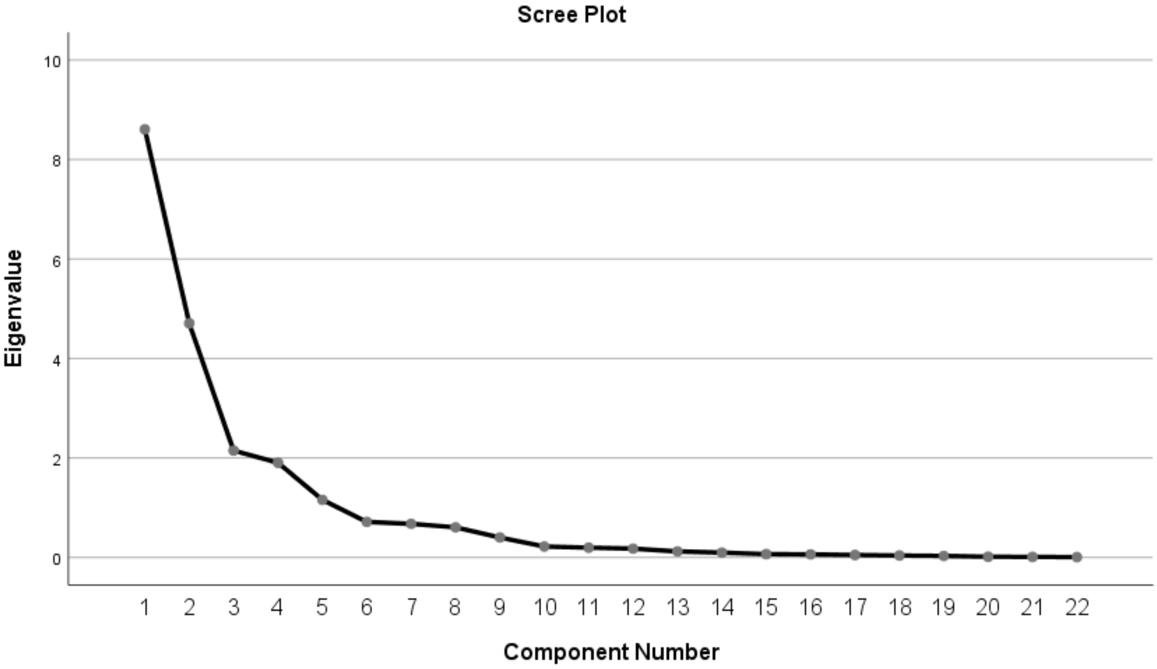
From the total variance explained table, it can be clearly seen that only four components had Eigen values of at least one. This therefore implies that the Principal Component Analysis had extracted 4 distinct factors from the data. Thus, the PCA extracted four key components for effective cyber risk management in SMEs. The total contribution of each factor to effective cyber risk management is shown in the '% of variance' column.

The findings shown in the table above show that 39.1% of effective cyber risk management is attributable to Factor 1, while Factor 2 contributed 21.4%, Factor 3 contributed 9.8% and lastly, Factor 4 contributed 8.7% to effective cyber risk management. The collective contribution of the four factors to effective cyber risk management was 78.93%. The remaining 18 components accounted for 21.1% towards effective cyber risk management.

4.3.4 The Scree plot

The scree plot shown in Figure 4.1 above is a line plot of the eigenvalues of factors or principal components extracted from the data (Lewith, Jonas, & Walach, 2010). The scree plot is used to determine the number of factors or principal components to retain in the principal component analysis (PCA).

Figure 4.1: The Scree plot

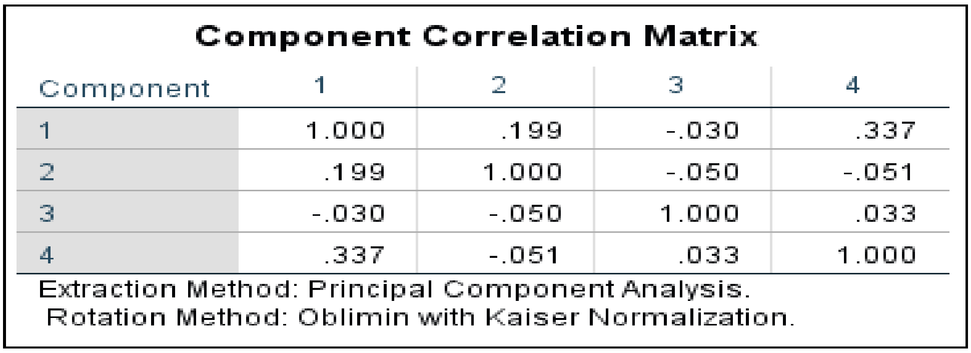


The researcher inspected the Scree plot to identify the principal components, that is those with Eigen values of at least 1. The Scree plot show that only 4 components have surpassed the value of 1 cut-off.

4.3.5 Factor Rotation

After determining the number of critical factors from the data, the study then went on to perform factor rotation to identify the factors. Having extracted the principal components from the data, the research undertook factor rotation. This involves the process on reorienting the factors so that low loadings become lower and high loadings larger. It is a mathematical procedure that rotates the factor axes in order to produce results that are more interpretable (Grande, 2016). It makes the loading patterns more clear, easier to identify and more pronounced. The study thus conducted a factor rotation in order to create a simple structure that can be interpreted. To determine the best rotation method, the study inspected the component correlation matrix. There are two key types of rotation i.e. orthogonal rotation and oblique rotation (Grande, 2016). The oblique rotation is employed if and only if there is at least one cross correlation coefficient whose absolute value has exceeded 0.35 (Grande, 2016). Consequently, an orthogonal rotation is appropriate if no cross-correlation coefficient in absolute value has exceeded 0.35. The component correlation matrix is shown in table 4.6 overleaf.

Table 4.6: Component Correlation Matrix



Component Correlation Matrix

Component	1	2	3	4
1	1.000	.199	-.030	.337
2	.199	1.000	-.050	-.051
3	-.030	-.050	1.000	.033
4	.337	-.051	.033	1.000

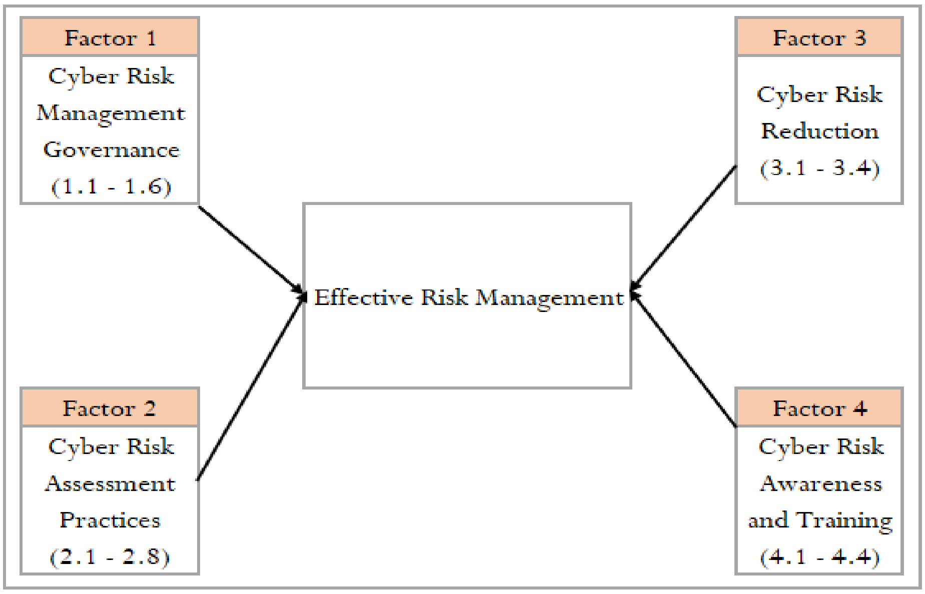
Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

Source: IBM SPSS Statistic version 25

From the table above, no absolute values exceeded 0.35, implying that no factor or component is significantly correlated to each other. These findings reveal that there is no problem of multicollinearity since the factors are not significantly correlated. As such, the principal components were uncorrelated, hence the orthogonal rotation was employed. Specifically, the study adopted the Varimax rotation procedure with Kaiser Normalization.

After extracting the principal components, the researcher used rotated component matrix to group and name the key factors as shown by the diagram below.

Figure 4.2: Rotated factors using Varimax


Factor 1
Cyber Risk Management Governance (1.1 - 1.6)
Factor 3
Cyber Risk Reduction (3.1 - 3.4)
Effective Risk Management
Factor 2
Cyber Risk Assessment Practices (2.1 - 2.8)
Factor 4
Cyber Risk Awareness and Training (4.1 - 4.4)

Source: IBM SPSS Statistic version 25

The findings in Figure 4.2 reveal that the critical factors for effective cyber risk management include risk governance, risk assessment practices, risk reduction practices and risk awareness and training. Furthermore, the findings revealed that the 22 items load together into four distinct constructs in a way where items 1.1 through to 1.6 stick together, items 2.1 to 2.8 load together, items 3.1 to 3.4 have factor loadings and items 4.1 through to 4.4 load together.

4.4 Checking for the existence of multicollinearity

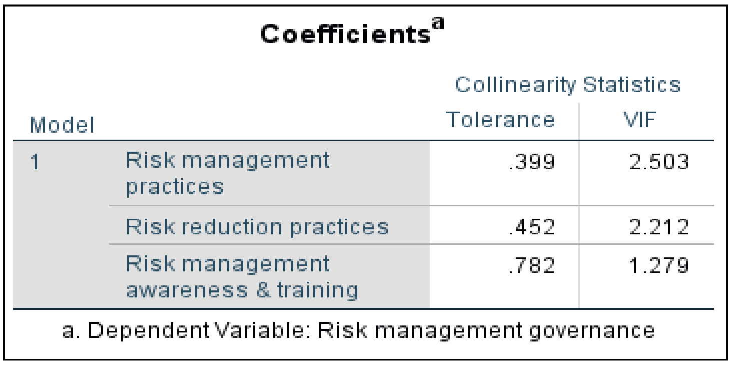
The results from the component correlation matrix in table 4.6 above show that the extracted factors are not correlated hence no multicollinearity. Fitting a model without checking for presence of multicollinearity would result in spurious regression results. Consequently, the study inspected the principal components for the existence of multicollinearity. To aid in the analysis, two statistics were also used to test multicollinearity of the predictor variables namely Tolerance Factor statistic and the Variance Inflation Factor (VIF) statistic.

4.4.1 Testing multicollinearity using Tolerance Factor statistic and the Variance Inflation Factor (VIF) statistic

The test procedure require that the Tolerance factor should be should be greater than 0.2 and its corresponding Variance Inflation Factor (VIF statistic) should be less than 5, thus confirming absence of multicollinearity.

Checking for collinearity: Factor 1 against other factors

Table 4.7: Collinearity Statistics



Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	Risk management practices	.399	2.503
	Risk reduction practices	.452	2.212
	Risk management awareness & training	.782	1.279

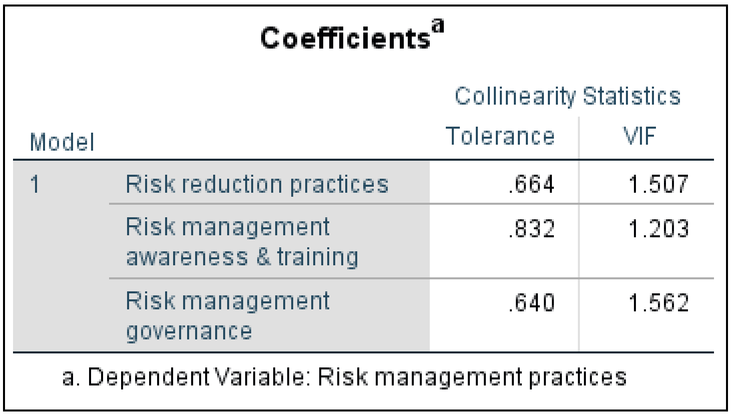
a. Dependent Variable: Risk management governance

Source: IBM SPSS Statistic version 25

From the multicollinearity diagnostics undertaken, it can be deduced that Factor 1, cyber risk governance is not significantly correlated with Factor 2, risk assessment practices (Tolerance = 0.399 > 0.2 and VIF = 2.503 < 5). Findings further showed no evidence of multicollinearity between Factor 1, cyber risk governance and Factor 3, cyber risk reduction practices (Tolerance = 0.452 > 0.2 and VIF = 2.212 < 5). There is no significant correlation between Factor 1, cyber risk governance and Factor 4, cyber risk awareness and training (Tolerance = 0.782 > 0.2 and VIF = 1.279 < 5).

Checking for collinearity: Factor 2 against other factors

Table 4.8: Collinearity Statistics



Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	Risk reduction practices	.664	1.507
	Risk management awareness & training	.832	1.203
	Risk management governance	.640	1.562

a. Dependent Variable: Risk management practices

Source: IBM SPSS Statistic version 25

From the findings of the multicollinearity diagnostics it can be deduced that Factor 2, cyber risk assessment practices is not significantly correlated with Factor 3, risk reduction practices (Tolerance = 0.664 > 0.2 and VIF = 1.507 < 5). Findings further showed no evidence of multicollinearity between Factor 2, cyber risk assessment practices and Factor 4, cyber risk awareness and training (Tolerance = 0.832 > 0.2 and VIF = 1.203 < 5). There is no significant correlation between Factor 2, cyber risk assessment practices and Factor 1, cyber risk governance (Tolerance = 0.664 > 0.2 and VIF = 1.507 < 5).

Findings shown by the two collinearity statistics in Tables 4.7 and 4.8 indicate that there is no multicollinearity among the factors since all factors are not significantly correlated to each other. The same result had been arrived at by checking the components correlation matrix in Table 4.6 above where it was seen that all correlations in absolute value were less than 0.35.

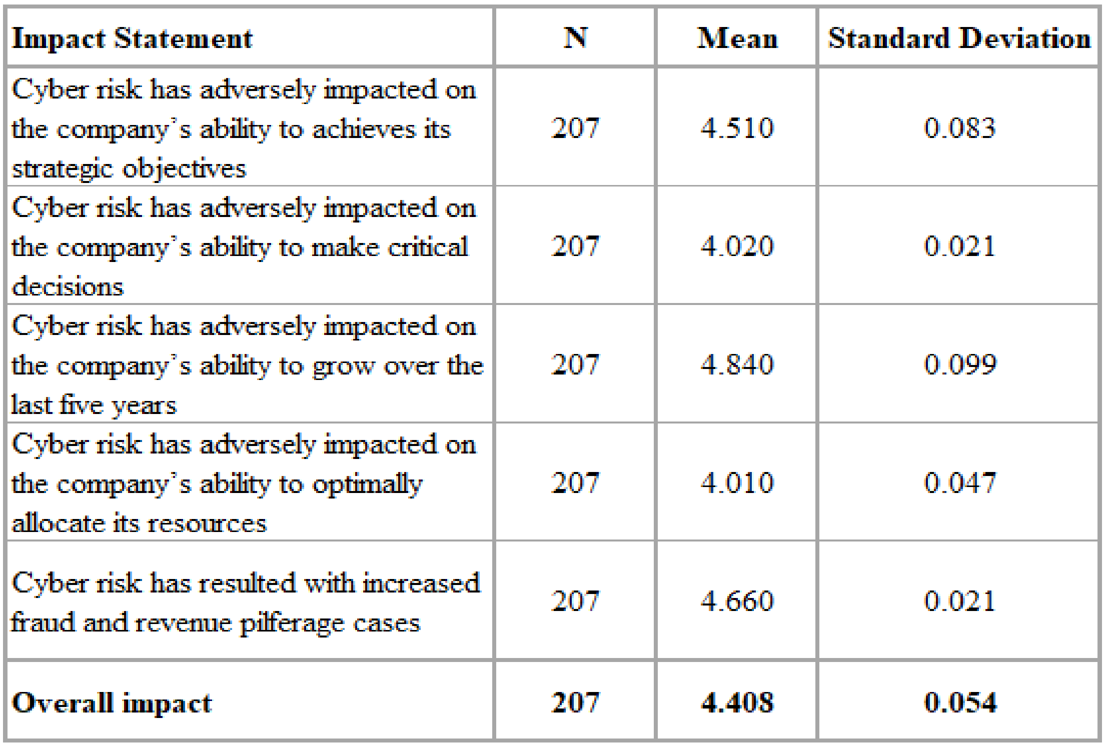
4.5 To examine the extent to which cyber risk has impacted on company performance

The second objective of this research was to evaluate the extent of the effect of cyber risk on performance of SMEs in Harare. To attain to this objective, the study sought to gather from the respondents their perceptions regarding the extent to which cyber risk has impacted performance of their companies. The researcher came up with a series of performance indicators and asked the respondents to show the extent to which these indicators are being affected by cyber risk. The performance indicators investigated include; firm's ability to attain to its strategic objectives, the company's ability to make critical decisions, the company's ability to grow, the company's ability to optimally allocate its resources and revenue pilferage.

The range of possible responses was 'no impact at all' (1) to 'to a very large extent' (5). The scores of no significant impact from cyber risk have been taken to represent a variable which had a mean score of 0 to lower than 2.5 on the continuous Likert scale. The scores of 'moderate extent' have been taken to represent a variable with a mean score of 2.5 to lower than 3.5 on the continuous Likert scale: and the score of both large extent and very large extent have been taken to represent a variable which had a mean score of 3.5 to 5.0 on a continuous Likert scale.

A standard deviation of greater than 0.9 implies a significant difference on the impact of the variable among respondents, while a standard deviation of less than 0.9 indicate the commonalities of views expressed by respondents on the measured variable (Uppal, Odhiambo, & Humphreys, 2005). To evaluate the extent of the impact posed by cyber risk on performance of SMEs, the researcher used both mean and standard deviation scores, as shown in the table overleaf:

Table 4.9: Effect of cyber risk on performance of SMEs



Impact Statement	N	Mean	Standard Deviation
Cyber risk has adversely impacted on the company's ability to achieves its strategic objectives	207	4.510	0.083
Cyber risk has adversely impacted on the company's ability to make critical decisions	207	4.020	0.021
Cyber risk has adversely impacted on the company's ability to grow over the last five years	207	4.840	0.099
Cyber risk has adversely impacted on the company's ability to optimally allocate its resources	207	4.010	0.047
Cyber risk has resulted with increased fraud and revenue pilferage cases	207	4.660	0.021
Overall impact	**207**	**4.408**	**0.054**

Source: IBM SPSS Statistic version 25

4.5.1 The effect of cyber risk on company strategic goals

The findings shown in Table 4.9 above reveal that the ability of SMEs to achieve their strategic objectives is being adversely affected by cyber risk. The majority of respondents, a mean score of 4.510 reveal that cyber risk has to a very large extent affected the company's ability to achieve its strategic goals. The corresponding standard deviation is 0.083 implying that majority of the respondents shared a similar view that Cyber risk has adversely impacted on the company's ability to achieves its strategic objectives. This result coincides with the findings of the studies performed by Gates et al. (2012) and Teoh and Muthuveloo (2015) who found that cyber risk negatively affects the organisation's long-term strategic objectives. SMEs are not spared from the effects of cyber risk as the global cost of cybersecurity breaches is expected to reach US$6 trillion in 2021 (Global Crime Report, 2017). The absence of strong cyber risk management structures within SMEs results in revenue losses through fraud or system downtime.

4.5.2 The effect of cyber risk on decision making

The findings shown in Table 4.9 above reveal that the ability of SMEs to make critical business decisions is being adversely affected by cyber risk. The majority of respondents, a mean score of 4.020 reveal that cyber risk has to a large extent affected the company’s ability to make crucial decisions which impact on business performance. The corresponding standard deviation is 0.021 implying that the majority of the respondents held a common position that Cyber risk has adversely impacted on the company’s ability to make critical decisions. This result is consistent with previous literature. Overby (2012) revealed that cyber risk if left uncontrolled can negatively affect company’s ability to make crucial decisions which impact on business performance.

4.5.3 The effect of cyber risk on company growth

Findings shown in Table 4.9 reveal a mean score of 4.840 and a corresponding standard deviation of 0.099 implying that the majority of the respondents perceived that cyber risk has to a very large extent adversely impacted on the company’s ability to grow over the last five years. The standard deviation indicates the commonalities of views expressed by respondents on the measured variable.

4.5.4 The effect of cyber risk on resource allocation

Findings shown in Table 4.9 above reveal that the ability of SMEs to optimally allocate their critical resources is being adversely affected by cyber risk. The majority of respondents, a mean score of 4.010 reveal that cyber risk has to a large extent affected the company’s ability to ensure optimal allocation of its resources. The corresponding standard deviation is 0.047 implying that the majority of the respondents held a common position that Cyber risk has adversely impacted on the company’s ability to achieve optimal allocation of its scarce resources. This result is supported by the findings of the study by Fielder *et al.* (2016) where it was revealed that exposure to cyber risk tends to affect the firm’s capacity to allocate its financial resources optimally.

4.5.5 The effect of cyber risk on fraud

The corruption indicators considered include fraud and revenue pilferage. The findings indicate that the majority of the respondents perceived that cyber risk has to a very large extent increased fraud and revenue pilferage cases. This is evidenced by a mean score of 4.660 and a standard deviation of 0.021. The overall statistics reveal that cyber risk has impacted on business performance to a large extent. This is supported by a mean score of 4.408 and the corresponding standard deviation of 0.054. The prevalence of cyber-criminals is a worrying development as

Zimbabwe grows more reliant on ICTs. More so, Moyo (2012) adds that, people cannot redefine fraud because it has been committed through cyberspace and further mentions that due to the fact that most victims of cybercrime are high-profile bank customers, they were reluctant to announce or admit in public that they have been successfully defrauded by some cyber-criminal. The same applies for small and medium firms who are not open to disclose fraud or security breaches to the general public, despite the fact that such an act would have negatively impacted on the financial resources and performance of the firm.

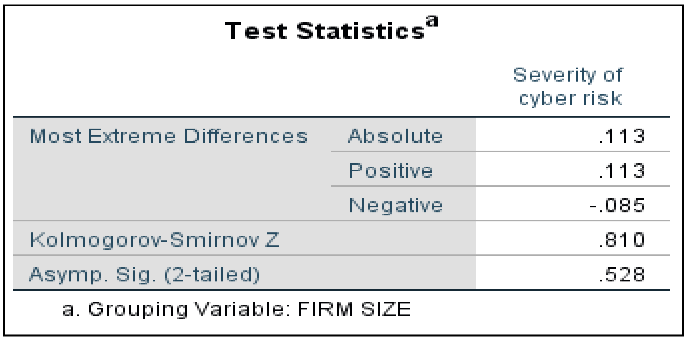
4.6 Establishing whether cyber risk severity depends on firm size

The study sought to ascertain the strength of cyber risk across firms of different sizes. The researcher allocated the SMEs into two mutually exclusive groups mainly, Small enterprises and Medium Enterprises. The criterion used to assign an individual firm into either a Small enterprises group or a Medium enterprises group was based on number of employees. Small firms are generally those with fewer than 50 employees, while medium-sized enterprises have employees ranging from 51-249 employees (OECD, 2005; Liberto, 2019; Amrin, 2018). The results are presented in the following sections:

4.6.1 Tests of independence

To assess whether there is independence of association between firm size and cyber risk intensity, the researcher adopted the independent samples t-test procedure to assess the independence of association between firm size and cyber risk intensity. The study variable cyber risk severity was identified to be normally distributed as shown overleaf.

Table 4.10: Kolmogorov-Smirnov Test



Test Statistics[a]

		Severity of cyber risk
Most Extreme Differences	Absolute	.113
	Positive	.113
	Negative	-.085
Kolmogorov-Smirnov Z		.810
Asymp. Sig. (2-tailed)		.528

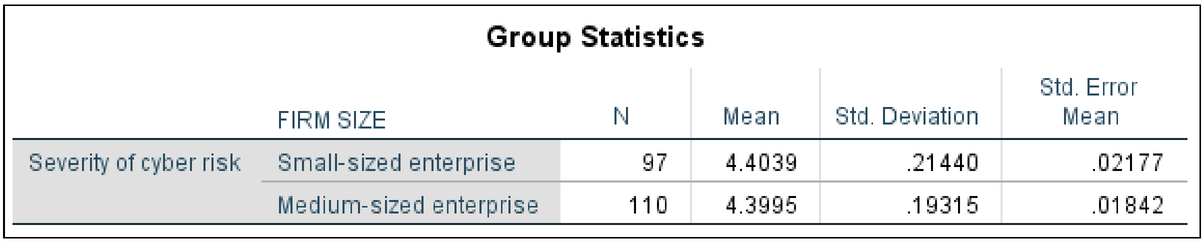
a. Grouping Variable: FIRM SIZE

Source: IBM SPSS Statistic version 25

Findings shown in Table 4.10 above indicate that the data for severity of cyber risk are normally distributed. This is supported by the asymptotic probability value (Sig.) of 0.528 which implies that the data are normally distributed. Since the data are normally distributed the researcher employed the independent samples t-test procedure.

4.6.2 Independent samples t-test

Table 4.11: Descriptive statistics



Group Statistics

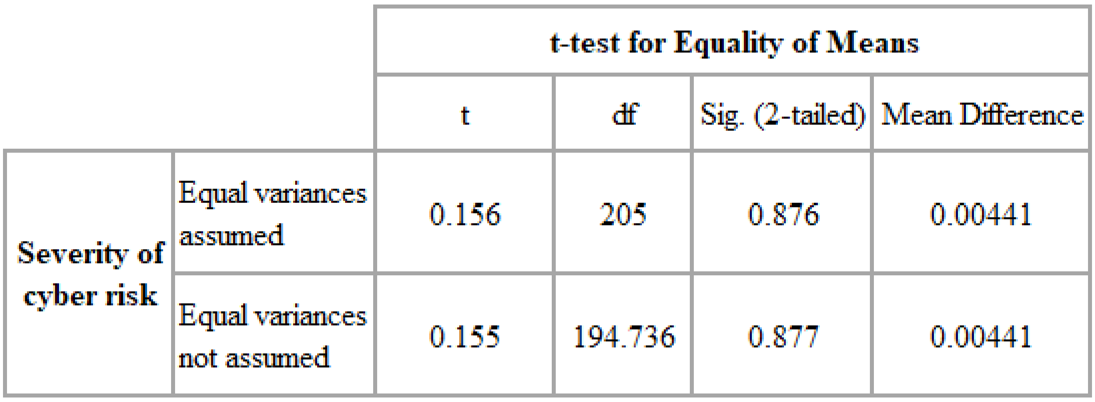
	FIRM SIZE	N	Mean	Std. Deviation	Std. Error Mean
Severity of cyber risk	Small-sized enterprise	97	4.4039	.21440	.02177
	Medium-sized enterprise	110	4.3995	.19315	.01842

Source: IBM SPSS Statistic version 25

From the group statistics table above, it can be deduced that the cyber risk has impacted to a large extent on performance of small-sized enterprises. This is evidenced by a mean score of 4.4039 and a standard deviation of 0.21440 implying that the majority of the small-sized firms suffer the same fate from cyber risk.

Similarly, from the group statistics table above it can be deduced that cyber risk has impacted to a large extent on performance of medium-sized enterprises. This is evidenced by a mean score of 4.4039 and a standard deviation of 0.19315 implying that the severity of cyber risk is equally shared among the majority of the medium-sized firms.

Table 4.12: Independent samples t-test



		t-test for Equality of Means			
		t	df	Sig. (2-tailed)	Mean Difference
Severity of cyber risk	Equal variances assumed	0.156	205	0.876	0.00441
	Equal variances not assumed	0.155	194.736	0.877	0.00441

Source: IBM SPSS Statistic version 25

The results of the independent samples t-test in Table 4.12 reveal that there is no significant difference between the severity/intensity of impact of cyber risk on firm size. Therefore, it can be concluded that at the conventional 5% level of significance there is sufficient evidence from the sample that severity of cyber risk does not significantly vary with respect to firm size. This therefore implies that the problem of cyber risk affects all firms regardless of whether they are small scaled or medium scaled.

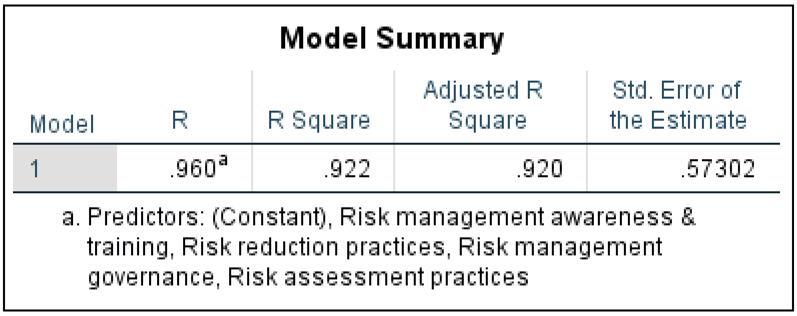
4.7 Establishing the effect of effective cyber risk management on firm performance

The fourth objective of the study was to establish the effect of effective cyber risk management on performance of SMEs. To attain this objective, the study employed multiple linear regression to determine the cause-and-effect relationship between the components of effective risk management and firm performance.

4.7.1 Regression analysis

Regression analysis considers the nature and form of a relationship between any two or more variables. Regression analysis was conducted on the data to quantify the effect of effective risk management on firm performance. Firm performance was measured in terms of firm's ability to achieve its strategic objectives, growth, optimal allocation of resources, improved decision making, stakeholder satisfaction and fraud decline. The results presented in Table 4.13 present the fitness of the regression model used in explaining this relationship.

Table 4.13: Model Summary



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.960[a]	.922	.920	.57302

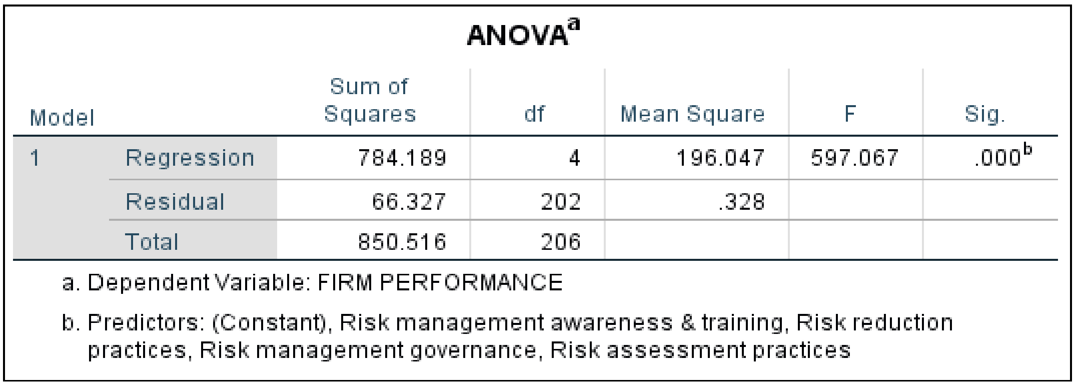
a. Predictors: (Constant), Risk management awareness & training, Risk reduction practices, Risk management governance, Risk assessment practices

Source: Author's compilation from IMB SPSS Statistic version 25

The independent variables which include cyber risk governance, risk assessment practices, risk reduction practices and risk awareness and training were found to explain 92.2% of changes in firm financial performance. This is supported by coefficient of determination also known as the R-square of 0.922. The coefficient of determination measures the proportion of the total variation in the dependent variable explained by the regression model. This results further means that the model applied to link the relationship of the variables was satisfactory.

Having established that the model explained 92.2% of the variance in the dependent variable, it was important to test whether this was statistically significant. Table 4.14 shows the ANOVA results.

Table 4.14: Analysis of Variance (ANOVA)



ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	784.189	4	196.047	597.067	.000[b]
	Residual	66.327	202	.328		
	Total	850.516	206			

a. Dependent Variable: FIRM PERFORMANCE

b. Predictors: (Constant), Risk management awareness & training, Risk reduction practices, Risk management governance, Risk assessment practices

Source: Author's compilation from IMB SPSS Statistic version 25

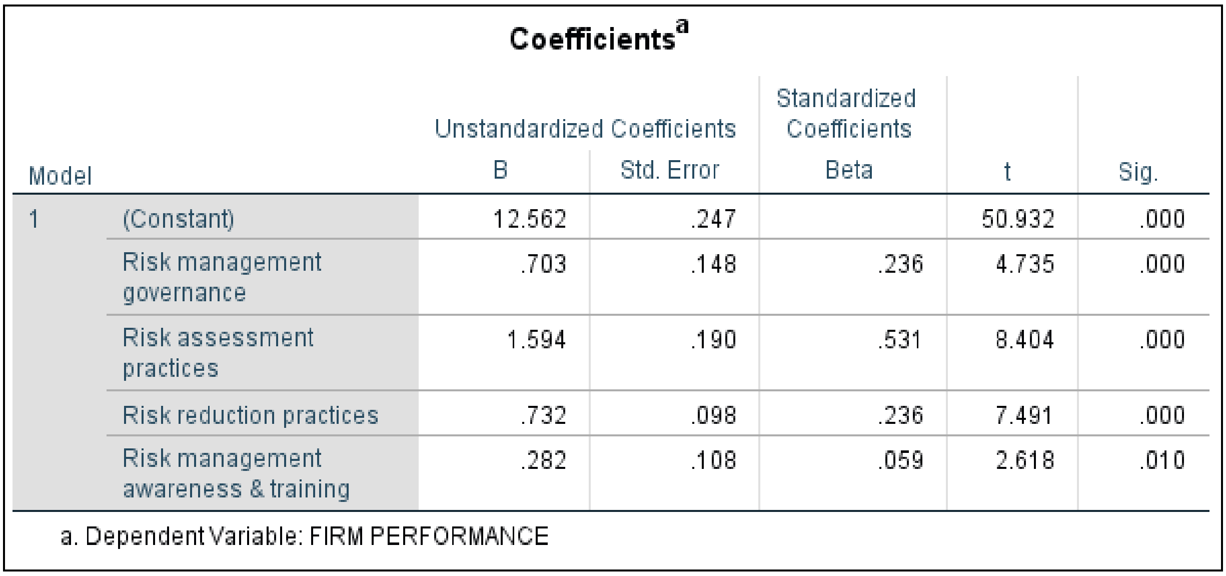
The assumed Null hypothesis is that there is no linear relationship between effective cyber risk management and firm performance (in other words $R^2 = 0$). The F-statistic is highly significant; thus, we can assume that there is a linear relationship between the variables in our model. The overall model was significant with an F statistic of 597.067. The F-value of the model produces a p-value of 0.000 which is essentially zero. A p-value of 0.000 is less than the set level of significance of 0.05 for a normally distributed data.

An assessment of the model fit is not enough to explain which of the variables in the model significantly impact on the dependent variable. This was accomplished through an analysis of regression coefficients below. From Table 4.15, using the beta coefficients of the independent variables, the model is:

$$Fp \ = \ 12.562 + 0.703(Rg) + 1.594(Ras) + 0.732(Rr) + 0.282(Rat)$$

Where *Fp* = *firm performance*
Rg = *Cyber risk governance*
Ras = *Cyber Risk assessment*
Rr = *Cyber risk reduction*
Rat = *Cyber risk awareness and training*

Table 4.15: Regression Analysis



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	12.562	.247		50.932	.000
	Risk management governance	.703	.148	.236	4.735	.000
	Risk assessment practices	1.594	.190	.531	8.404	.000
	Risk reduction practices	.732	.098	.236	7.491	.000
	Risk management awareness & training	.282	.108	.059	2.618	.010

a. Dependent Variable: FIRM PERFORMANCE

Source: Author's compilation from IMB SPSS Statistic version 21

The study finds a positive and statistically significant impact of risk governance on firm performance (β=0.236, p=0.000<0.05). This indicates that holding other factors constant, a 1-unit increase in good risk governance for cyber security is associated with a 0.236 unit increase in organizational performance. Risk assessment practices showed a positive (β=0.531) and statistically significant (p=0.000<0.05) relationship with firm performance. This indicates that holding other factors constant, a 1-unit increase in the use of risk assessment practises is associated with a 0.531 unit increase in firm performance.

The study also finds a strong positive relationship between Risk reduction practices and firm performance (β=0.236, p=0.000<0.05). One unit increase in risk reduction practices is predicted to increase firm performance by 0.236 units holding other factors constant. Finally risk awareness and training is positively (β=0.059) and significantly related with firm performance (p=0.010<0.05). Of all the constructs, risk assessment practices has the greatest impact on firm performance (β=0.531).

4.8 Discussion of Findings

This study sought to understand on the impact of cyber risk management on corporate performance of SMEs in Harare. Presented in the sections below are the discussions regarding the hypothesis and comparison of the study finds to current literature.

The results agree with empirical literature. Jenya and Sandada (2017) conducted a study to investigate the impact of the 5 main processes of the COSO ERM framework on the performance of SMEs. The study found a positive and significant relationship between Effective Risk Management (ERM) and the performance of SMEs (Jenya and Sandada, 2017). Similarly, Teoh, Lee and Muthuveloo (2017) found a statistically significant relationship between ERM implementation and firm performance in Malaysia. Teoh and Muthuveloo (2015) investigated the impact of ERM on corporate performance in public listed companies in Malaysia and the study found a positive and significant association between the implementation of ERM and firm performance.

The study results however differ with the findings of the study by Alawattegama (2018) who assessed the impact of ERM on the performance of financial services firms, Sri Lanka and the study revealed that none of the eight key ERM functions as suggested by the COSO ERM integrated framework has a significant impact on firm performance.

These results indicate that cyber risk governance, if adopted by SMEs, will positively impact business performance. These results are consistent with findings of a study by Ridley et al. (2004) who concluded that IT risk governance is a good practice which positively contributes towards enhanced business performance. These results show SMEs should take time to set proper governance structures and clear operational policies and objectives to identify and mitigate cyber risks arising its people, systems and procedures and from other corporates that it deals with. The starting point can be having a dedicated resource responsible for identifying, monitoring and reporting cyber threats in the SMEs. Due to limited financial resources within SMEs, such a role can also assume additional responsibilities within the firm.

The second specific study hypothesis (H2) was that cyber risk assessment practices positively and significantly influences businesses performance. The study results are consistent with the

Agency theory, which posits that risk assessment practices are necessary to mitigate the different interests of agents and principals in an organisation thereby increasing stakeholder commitment which in turn improves business performance (Smith and Stulz, 1985). Furthermore, Yang and Anwar (2018) conducted a study to evaluate the impact of Effective Risk Management among SMEs in Pakistan, where it was established that effective risk assessment practices positively impact on both performance and competitive advantage of SMEs. From the study, it was evident that SMEs are using varied technological enablers within their business. In most cases, these tech enablers usually have inbuilt mechanisms to monitor network activities and unauthorised access, when properly configured. It is therefore important that SMEs that advantage of some of these product features to continuously assess cyber risks. Furthermore, as new products or partners are onboarded, SMEs should also assess the resultant level of risk which such an activity has brought and be appropriately reviewed against its risk tolerance levels of the company.

The results are in support of the hypothesis statement H3 that cyber risk reduction practices positively and significantly impact on business performance hence the hypothesis was accepted. These results indicate that cyber risk reduction practices are boosting business performance. Risk reduction results for SMEs might mean communication with external stakeholders so that they also enhance their cyber risk management practises in their operations. That way, risk is managed by each party reducing exposure to others. Risk transfer can also be applied by SMEs where an insurance policy is taken to cover against risk such as business disruption and system failure (e.g. loss of productive time) in the business resulting in improved operation performance. From the survey, most of the responded indicated that they were not aware that insurance can be taken against such threats. This presents a great opportunity for insurance company to market their insurance products to this sector.

These results indicate that cyber risk awareness & training positively contribute towards improved business performance. These results are in support of the findings by Ridley et al. (2004) who concluded that intensifying risk management awareness and training is a good practice which contributes significantly towards enhanced business performance. In the study, respondent highlighted little to no cyber risk training or awareness programs by their employers. In the management of cyber risk, awareness is usually the first step towards taking responsibility. With the right training and information, SMEs will be equipped with the right skills and knowledge to identify, assess, monitor and report on the cyber risks they face. Employees who are not aware end up unwittingly accepting high level of risk which negatively impacts on the performance of the business.

4.9 Managerial Implications

Due to the huge contribution to global income, SMEs are very important in the economy of all countries in the world. SMEs should have and apply security policy related to technology, procedures and people. This work demonstrates that good risk management governance tends to boost business performance, hence management should enforce good cyber risk management governance.

SMEs should not run outdated business software and antivirus software. Moreover, they ought to receive and utilize encryption software, digital signatures, email authentication, policy and reporting protocol. Business owners should take a look at their data and processes to see how well protected they are. Other recommendations include: providing staff with access to simple, freely available cyber security training and taking regular cyber security risk assessment on all facets of the business's operations.

4.10 Chapter Summary

The chapter presented results on the impact of key components of effective cyber risk management on business performance. It was found that governance, risk assessment strategies, risk reduction strategies and risk awareness and training positively and significant impact on business performance. The following chapter focusses on summary of findings, conclusions and policy recommendations.

Chapter 5: Summary of Findings, Conclusions and Recommendations

5.1 Introduction

The subsequent sections in this chapter presents the achievement of research aim and objectives, conclusions, answer to research questions, contributions, recommendations, generalisation of findings and research limitations based on the findings of the study. Section 5.2 highlights the initial aim and objectives of the study as well as its rationale. Section 5.3 focusses on the conclusions of the study, while section 5.4 outlines the theoretical, methodological and empirical contributions of the research. Section 5.5 focuses on policy recommendations while section 5.6 focusses on managerial recommendations. Generalisation of findings are covered in section 5.7. The chapter culminates by presenting the limitations of the study in section 5.8.

5.2 Achievement of research aim and objectives

The study sought to examine the impact of effective cyber risk management practices on performance of SMEs in Harare, Zimbabwe. The results indicate a meaningful impact of effective cyber risk management on business performance. Therefore, any improvements made to effective cyber risk management tend to enhance business performance.

The main research objective of the study was to ascertain the impact of effective cyber risk management on performance of SMEs. To attain this objective, the study conducted an analysis of variance (ANOVA) where the results indicated that effective cyber risk management impacted significantly on business performance.

The first specific objective of this study aimed at identifying, extracting, rotating and isolating the principal components of effective cyber risk management. To attain this objective, the study sought the respondent opinions concerning how SMEs are managing strategic risks. The researcher conducted factor analysis in order to determine the key components of effective cyber risk management in SMEs. The questionnaire had 22 distinct items or questions (also called variables) and each question was ordinally scaled with response categories ranging from 1 through to 5 on a Likert scale. The researcher employed factor analysis to identify the number of critical components required in explaining cyber risk management. Results of the Principal Components Analysis (PCA) reveal that the critical components for effective cyber risk management include risk governance, risk assessment practices, risk reduction practices and risk management awareness and training.

The second objective of this research was to evaluate the extent to which cyber risk affected performance of SMEs. To attain this objective, the study sought to get from the respondents, their perceptions on the extent to which cyber risk has impacted on the performance of their businesses. The researcher came up with a series of performance indicators and asked the respondents to show the extent to which these indicators were being affected by cyber risk.

The findings reveal that cyber risk has adversely affected the ability of SMEs to achieve their strategic objectives. The results also show that the ability of SMEs to make critical business decisions was adversely affected by cyber risk. Furthermore, the findings revealed that cyber risk has to a very large extent negatively impacted on the company's ability to grow. The presence of cyber risk also negatively impacted on resource allocation by SMEs.

The third objective study sought to ascertain the strength of cyber risk across firms of different sizes. To achieve this objective, the researcher started by allocating the SMEs into two mutually exclusive groups mainly, Small Enterprises and Medium Enterprises. The criterion used to assign an individual firm into either a Small enterprises group or a Medium enterprises group was based on number of employees. Small firms are generally those with fewer than 50 employees, while medium-sized enterprises have employees ranging from 51-249 employees (OECD, 2005; Liberto, 2019; Amrin, 2018). To assess whether there is independence of association between firm size and cyber risk intensity, the researcher adopted the independent samples t-test procedure to assess the independence of association between firm size and cyber risk intensity. The results of the independent samples t-test revealed that there was no significant difference between the severity/intensity of cyber risk on firm size. This therefore implies that cyber risk affects all SMEs regardless of size.

The fourth objective of the study was to establish the impact of cyber risk management drivers on firm performance. To attain to this objective, the study fitted a regression model where the magnitude and direction of factor effect was determined from the value of the regression coefficient and its sign respectively. On the other hand, the significance of the factor effect was determined by the probability value (p value) corresponding to the factor coefficient. With reference to the impact of cyber risk reduction practices, results indicate that cyber risk reduction practices have a positive and statistically significant impact on business performance. The study culminated by testing the impact of awareness and training on firm performance. The study results further indicated that cyber risk management awareness and training have a positive and statistically significant impact on business performance.

5.3 Conclusions

Based on the study findings, the following conclusions were made:

5.3.1 Effective cyber risk management positively impacts on business performance

The main hypothesis of the study was that effective cyber risk management significantly impacts on performance of SMEs. The results indicate a meaningful impact of effective cyber risk management on business performance. It can therefore be inferred that at 5% level of significance, there is sufficient evidence from the sample that the implementation of effective cyber risk management positively impacts on business performance. The study therefore concludes that SMEs that implement cyber risk management are expected to see improvements in performance in terms of better resource allocation, operational excellence and consistency in achieving set strategic objectives. As such, the findings support studies by Allawattegama (2018) and adds to the literature on cyber risk management by SMEs.

5.3.2 Governance of cyber risk positively and significantly impacts business performance

The results indicate that risk governance has a positive and statistically significant impact on business performance. The results are in support of the hypothesis statement H1 that improved cyber risk management governance tend to improve business performance, therefore the hypothesis was accepted. It can therefore be concluded from the study findings that at the conventional 5% level of significance there is sufficient evidence from the sample data that cyber risk governance is critical for boosting SMEs performance. It was established that appropriate cyber risk governance structures to a greater extent improve business performance as both senior management and employees are made aware and act on the cyber risks they face, thus improving operations.

5.3.2 Cyber risk assessment practices positively and significantly impacts business performance

Risk assessment practices have a positive and statistically significant impact on business performance which strongly supports the hypothesis. It can therefore be concluded from the study results that at 5% level of significance there is sufficient evidence from the sample data that the implementation of Cyber risk assessment practices by SMEs positively impacts on their business performance. Structured cyber risk assessment will set tone regarding how management will react to the risk they faced, thus feeding the results of the assessment into decision making by those charged with governance of the SME. Such a process would result in better decision making and improvements in SME performance. As such, risk management opens the way for the other cyber risk management measures to be effect by management. Without the assessment, SMEs will be shooting in the dark regarding real and potential risks they face.

5.3.4 Cyber risk reduction practices positively and significantly impacts performance

The results indicate that cyber risk reduction practices have a positive and statistically significant impact on business performance. The results are in support of the hypothesis statement H3 that cyber risk reduction practices positively and significantly impact on business performance hence the hypothesis was accepted. The hypothesis is accepted and it can be concluded that at 5% level of significance there is sufficient evidence from the sample data that the implementation of Cyber risk reduction practices by SMEs tend to positively impact on their business performance. Risk reductions should assist the SMEs in reducing the cyber risks identified at the assessment management, thus bringing it to acceptable levels by the business.

5.3.5 Cyber risk management awareness and training positively and significantly impacts business performance

The results indicate that cyber risk management awareness and training has a positive and statistically significant impact on business performance. The results are in support of the hypothesis statement H4 that improved cyber risk awareness and training on SMEs tend to improve business performance, therefore the hypothesis was accepted. The hypothesis is accepted and it can be concluded that at 5% level of significance there is sufficient evidence from the sample data that efforts to ensure cyber risk management awareness and training tend to positively impact on performance of SMEs. Managing cyber risk first requires an understanding that such risks exists. SMEs should invest in training and awareness programs for their employees. Such programs will also have the impact of equipping the employees with skills required to identify, assess, monitor, report and manage the cyber risks faced by the SMEs.

5.4 Contributions

This study sought to add literature to the pool of available knowledge about the influence of effective cyber risk management on corporate performance of SMEs in Harare. Presented in the sections below are theoretical contributions, methodological contributions, empirical contributions and policy recommendations:

5.4.1 Theoretical contribution

Currently, there is a relatively scanty research on the impact of components of effective risk management on firm performance in the context of cyber risk. This study fills this gap by providing first hand data and empirical analysis on the impact of effective cyber risk management on SMEs performance. The findings of this study will not only add to the literature on SMEs performance but also provide relevant empirical literature that can also be used not only for SMEs but even when studying cyber risk management in big corporates. The study results also validated the suggestions of the agency theory which posits that risk assessment practices are necessary to mitigate the different interests of agents and principals in an organisation thereby increasing stakeholder commitment which in turn improves business performance (Smith and Stulz, 1985).

5.4.2 Methodological contribution

The methodological contribution of this study is the adoption of factor analysis specifically the Principal Components Analysis (PCA) in factor extraction. Previous studies used different methodologies. A study that was conducted by Polkowski & Dysarz (2017) conducted a study on IT Security Management in Small And Medium Enterprises. This study used frequencies and descriptive statistics to assess the impact of IT risk management in SMEs without first extracting the potential factors from the data. Polkowski & Dysarz (2017) worked with information contained in a large number of variables which could have been loaded into a smaller number of subsets or factors through principal components analysis. The justification for adopting the factor analysis was based on several benefits of using PCA. Factor analysis is a multivariate statistical technique that is used to summarize the information contained in a large number of variables into a smaller number of subsets or factors. The study employed the factor analysis primarily in order to simplify the data and to group together variables which are heavily correlated in distinct constructs called principal components.

5.4.3 Empirical contribution

The results of the study validated the findings of previous studies. The study has provided a basis upon which policy makers can determine the best possible ways of assisting SMEs on improving their performance. By conducting the research in the Zimbabwean context enabled the policy markers to get insights on the key components of effective cyber risk management in the SMEs context.

5.5 Policy recommendations

The policy makers will significantly immensely from the study findings, as it provides a baseline and advocates for the adoption and continued used of modern technology by SMEs. The CZI laments low adoption of technology by corporates, with latest reports showing that only 16% have invested in modern technology. The study will enable policy makers to come up with strategies that motivate SMEs to embrace rather than fear information communication in general, at the same time ensuring that robust cyber risk structures are put in place, thereby positively impacting on performance and contribution of the SMEs to the Zimbabwean economy.

Furthermore, there is consensus amongst SMEs that adoption of technology has opened them up to cyber risk. As there is no law currently governing the cyber space, this risk continues to become significant. The government, in response to security concerns mainly of political nature, have instituted the cyber security bill which is currently at hearing stage. This study recommends that the bill be reviewed and strengthened to provide wide protection for business and corporates alike in a networked and digital era.

5.6 Managerial recommendations

The research findings highlight that SMEs that invest time and money into cyber risk management are predicted to perform better than their competitors. The relationship between cyber risk management and corporate performance is summed up by the following regression equation:

$$Fp = 12.562 + 0.703(Rg) + 1.594(Ras) + 0.732(Rr) + 0.282(Rat)$$

The study therefore makes the following practical recommendations to executives of SMEs:

a) Companies should upskill their employees with cyber risk management skills

With the fast pace through which technology is becoming a key enabler in business, cyber risk management will become a key skills requirement for all employees. The exposure brought by cyber risk can result in the business losing its valuable proprietary assets. In light with the finding that cyber risk management is beneficial for improved performance, this study recommends that companies should invest in upskilling their staff to identify cyber risk exposures in business operations and build awareness on the nature of risks the company is exposed to.

b) SMEs should invest in cyber risk environmental scanning tools

This study has shown that environmental scanning for through cyber risk management positively impact on organizational performance. This study therefore recommends that companies invest resources into software's and platforms that help them to do data mining and analytics based on cyber risk information. This will assist the companies to develop products that meets the ever changing customer needs and preferences while also fending off risk exposures brought by technology use.

c) SMEs should enforce good risk governance in their operations

Due to the huge contribution to global income, SMEs are very important in the economy of all countries in the world. SMEs should have and apply security policy related to technology, procedures and people. This work demonstrates that good cyber risk governance tends to boost business performance hence management should enforce good cyber risk governance within their operation. SMEs shouldn't run outdated business software and antivirus software. Moreover, they ought to receive and utilize encryption software, digital signatures, email authentication, policy and reporting protocol.

d) SMEs should ensure presence of sound application and physical security around their assets

Business owners should take a look at their data and processes to see how well protected they are. General access rules organizations' internal network and thus all devices and assets connected within should be protected against unauthorized access. Using firewalls or equivalent solutions is essential. The default administrator password for any firewall should be changed to an alternative, strong password. This rule is a valid for passwords in general. The quality of a password is dependent on the number of characters, the types of characters, type of algorithm and the quality of the hardware that is attempting to break the password. Other recommendations include: providing staff with access to simple, freely available cyber security training and taking a cyber security risk assessment.

e) SMEs should formalise and document their cyber risk management policies

More specifically, SMEs further need to invest time and money in documenting their cyber risk management policies and practices. SMEs are currently face by issues of frauds, data challenges, and uncollectable debtors book among other problems which impact on sustainable performance. As such, business owners and executive should establish cyber risk management policies with clear risk tolerance levels and operational strategies to manage cyber risks arising its people, systems and corporates they deal with. Furthermore, the said policies should be complemented with a sound framework of internal controls.

5.7 Generalization of findings

After using the Principal Component Analysis (PCA), it was identified that the key components for effective cyber risk management include; risk governance, risk assessment practices, risk reduction practices and risk management awareness & training. These key factors were investigated through regression analysis and it was identified that they all positively and significantly impacts business performance.

5.8 Research limitations

Like any piece of research, this review paper has limitations, which are to be acknowledged. This study did not include risk identification strategies and risk analysis strategies which are considered to be critical factors for effective risk management (Falkner, 2015).

However, the study did not include risk identification and analysis solely because it is not yet clear who contributes to risk identification and analysis in SMEs; is it only the SME owners/managers, or do they also seek outside advice – and if so, what is the impact of external advice on the risk management practices in SMEs?

Finally, since this study focused exclusively on the SME sector, further studies can be initiated on other industries applied to other industries and economic sectors to investigate the impact of these cyber risk dimensions on corporate performance.

References

Abor, J., and Quartey, P., (2010). Issues of SMEs development in Ghana and South Africa, International Journal of Finance and Economics, 2 (8): 1 – 14

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S. and Upton, D. (2018), "A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate", Journal of Cybersecurity, Vol. 4 No. 1.

Agwu, O. M., and Emeti, I. C., (2014). Issues, challenges and prospects of small and medium scale enterprises (SMEs) in Port-Harcourt city, Nigeria. European Journal of Sustainable Development, 3, 1, 101-114

Alawattegama, K. K. (2018). The Impact of Enterprise Risk Management on Firm Performance: Evidence from Sri Lankan Banking and Finance Industry. International Journal of Business

Albu C. N, and Klimczak K. M., (2017). "Editorial. Small and Medium-Sized Entities Reporting In Central and Eastern Europe," Journal of Accounting and Management Information Systems, Faculty of Accounting and Management Information Systems, The Bucharest University of Economic Studies, vol. 16(2), pages 221-228, June.

Alexander, G. J., (2009). From Markowitz to modern risk management. *The European Journal of Finance*, 15, (5), 451–461.

Ambrož M., (2012). "Security Culture Impact on Security Excellence in a Company". Innovative Issues and Approaches in Social Sciences, vol.5, no.1:70-87.

Amrin, N., (2018). The Impact of Cyber Security. SAGE Journals, 1-77.

Asti, A., (2017), "Cyber defense challenges from the small and medium sized business perspective", SANS Institute, InfoSec Reading Room, available at: www.sans.org/reading-room/whitepapers/ hsoffice/paper/38160 (Accessed 21 December 2019).

Ayyagari, M., Demirguc-Kunt, A., and Maksimovic, V. (2016). Small vs young firms across the world: contributions to employment, job creation, and growth, Policy Research Working Paper 5631. World Bank, DC, Washington

Bada, M., Sasse, A.M. and Nurse, J.R.C. (2015), "Cyber security awareness campaigns: why do they fail to change behaviour?", The International Conference on Cyber Security for Sustainable Society, SSNþ, pp. 118-131.

Baxter, R., Bebard, J. C., Hoitash, R. and Yezegel, A. (2013). Enterprise Risk Management Program Quality: Determinants, Value Relevance and the Financial Crisis. *Contemporary Accounting Research*, 30(4), 1264-1295.

Beasley, M. S., Pagach, D., and Warr, R. (2008). The information conveyed in hiring announcements of senior executives overseeing enterprise-wide Risk Management process. *Journal of Accounting, Auditing and Finance*, 23(3), 11-332.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28, str. 24-31. Doi: https://doi.org/10.1016/S2212-5671(15)01077-1

Berg, B., (2010), Qualitative Research Methods for the Social Sciences, Pearson, London.

Böhme, R., and Kataria, G., (2006): Models and Measures for Correlation in Cyber-Insurance, Working Paper, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK.

Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L.: The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. Comput. Secur. 11(3), 431–448 (2003)

Carter, D.A., Rogers, D.A. and Simkins, B. J. (2006). Hedging and value in the U.S. Airline Industry. *Journal of Applied Corporate Finance*, 18(4), 21-33.

Casualty Actuarial Society (CAS, 2003). http://www.casact.org/ (Accessed 20 December 2019)

Cavusoglu, H., et al, "A Model for Evaluating IT Security Investments," Communications of the ACM, vol. 47, no. 7, 2004

Cebula, J. J., and Young, L. R., (2010): A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

CERT 2013 US State of Cybercrime Survey, Available: http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf, (Accessed 04 November 2019)

CIPESA (2017). “Bridging cyber security gaps: SMEs trained in Uganda”, available at: https://cipesa. org/2017/09/bridging-cyber-security-gaps-smes-trained-in-uganda/ (Accessed 14 November 2019).
Contos, B. (2015), “Cyber security culture is a collective effort”, IDG Contributor Network.

Chia, K., (2005). “Singapore”, in Campbell, D. (Ed.), E-commerce and the Law of Digital, Oxford University Publishers, London.

Cost of Cyber Crime Study: Global Report (2013). Available: http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports. Last Accessed: 12/11/2019

De Brun , K.G., Maitland, A. and Bianchi, S.M., 20069. Nonresponse in the American time use Survey: Who is missing from the data and how much does it matter? International Journal of Public Opinion Quarterly, 70(5), pp.676-703.

Deloitte., (2012). Aftershock: Adjusting to the New World of Risk Management. London: Deloitte Development LLC

Dojkovski, S., Lichtenstein, S. and Warren, M.J. (2017), “Fostering information security culture in small and medium size enterprises: an interpretive study in Australia”, ECIS, pp. 1560-1571.

Eling, M., and Schnell, W., (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), str. 474-491. Doi: https://doi.org/10.1108/JRF-09-2016-0122 (Accessed 31 December 2019).

ENISA, (2019). “Cybersecurity culture guidelines: behavioural aspects of cybersecurity”, available at: www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/ (Accessed 31 January 2020).

European Commission, 2003. ‘Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium sized enterprises’, Official Journal of European Union, 46 (May 20): 36-41.

Falkner, E. M., (2015). Risk management in SMEs: a systematic review of available evidence. Journal of Risk Finance, 2-32.

Faff, R., and Nguyen, H., (2002). On The Determinants of Derivative Usage by Australian Companies. *Australian Journal of Management*, 27(1), 1-24.

Fielder A., Panaousis E., Malacaria P., Hankin C., and Smeraldi F., 2016. “Decision support approaches for cyber security investment,” Decision Support Systems, vol. 86, pp. 13–23.

Florio, C., and Leoni, G., (2017). Enterprise Risk Management and Firm Performance: Italian Case. *The British Accounting Review*, 56-74.

Fatt, E.K., and Wahjanto, A., (2005). “Malaysia”, in Campbell, D. (Ed.), E-commerce and the Law of Digital Signatures, Oceana, Dobbs Ferry, NY, pp. 427-448.

Furnell, S., and Thomson, K.L., (2009). “Recognising and addressing ‘security fatigue’”, Computer Fraud and Security, Vol. 2009 No. 11, pp. 7-11.

Gambanga, N., (2016). Guilty of spam? – here are 13 offences in Zimbabwe’s draft Computer Crime & Cybercrime Bill. Retrieved from TechZim Web site: http://www.techzim.co.zw/2016/09/guilty-spam-13-offences-zimbabwes-draft-computer-crime-cybercrime-bill/ (Accessed 2 December 2019)

Gates, S., Jean-Louis, N. and Walker, P. L. (2012). Enterprise Risk Management: A process for enhanced management and improved performance. Management Accounting Quarterly, 13(3), 28-38. https://hal.archives-ouvertes.fr/hal-00857435 (Accessed 10 December 2019).

Géczy, C., Minton, B. A., and Schrand, C. (1997). Why Firms Use Currency Derivatives. *The Journal of Finance*, *52*(4), pp 1323-1354.

Global Entrepreneurship Monitor (2014). Website https://www.gemconsortium.org/report/gem-2014-global-report

Global Risks Report 2017, The World Economic Forum, 11 January 2017.

Goel R., Haddow J., and Kumar A., 2018: Managing Cybersecurity Risk in Government: An Implementation Model. Accessed at www.businessofgovernment.org on 7 November 2019.

Graham, J. and Rogers, D. (2002). Do firms hedge in response to tax incentives? *Journal of Finance*, 57(2), 815-839.

Grande. R, (2016). Selecting a Rotation in a Factor Analysis using SPSS: Mar 3, 2016. New Delhi: YouTube: https://www.youtube.com/watch?v=nIv8h4rQ7K4. (Accessed 11 January 2020)

Griffiths, D.H., and Harrison, J., (2005). “United Kingdom”, in Campbell, D. (Ed.), E-commerce and the law of Digital Signatures, Oceana, Dobbs Ferry, NY, pp. 151-174.

CRO Forum: Cyber Resilience – the cyber risk challenge and the role of insurance. 2014 (9.5.2017) http://www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf (Accessed 18 November 2019).

Hair, J. F., Black. W.C., Babin, B. J. and Anderson, R. E. (2010). *Multiple Data Analysis*. Upper Saddle River, 7 7th ed. Pearson Prentice Hall.

Hathaway, M., Demchak, C., Kerben, J., Jennifer, M., and McArdle, F. (2015). Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index. Arlington, VA: Potomac Institute for Policy Studies

Heale, R., and Twycross, A., (2015). Validity and reliability in quantitative studies. *Evidence Based Nursing,* 18 (3), pp 66-67

Hovay, A., and D'Arcy, J. (2003): The impact of denial-of-service attack announcements on the market value of firms. Risk. Manage.Insur. Rev. 6(2), 97–121

Hoyt, R.E., and Liebenberg, A.P., (2011). The value of enterprise risk management: *The Journal of Risk and Insurance,* 78(4), 795-822.

InfoSecurity (2017), "UK SMEs still do not educate their staff on the risk of cyber security", available at: www.infosecurity-magazine.com/news/uks-smes-failing-on-cyber-training/ (Accessed 21 January 2020).

Institute for Risk Management South Africa (2014). The IRMSA Guideline to Risk Management. https://www.irmsa.org.za/ [Retrieved 15 November 2019.]

Insurance Journal, (2018). Website: https://www.insurancejournal.com/news/international/-2018/02/16/480919.htm (Accessed 12 December 2019)

ISACA (Information Systems Audit and Control Association), 2012a. COBIT 5: A business framework for the governance of enterprise IT. Rolling Meadows, IL.

Iuga, C., Nurse, J.R.C. and Erola, A. (2016), "Baiting the hook: factors impacting susceptibility to phishing attacks", Human-Centric Computing and Information Sciences Journal, Vol. 6 No. 1, pp. 8-20.

Jensen, M.C., and Meckling, W.H., (1976). Theory of firm: Managerial behaviour, agency cost and ownership structure. *Journal of Financial Economics* 3(4), 305-360.

Jenya, B., and Sandada, M., (2017). Enhancing Success of SMEs through Risk Enterprise Management: Evidence from a Developing Country. *Pakistan Journal of Applied Economics, 27(2),* 173-188

Jin, Y., and Jorion, P., (2006). Firm value and hedging: Evidence from U.S. Oil and Gas Producers. *Journal of Finance* 61(2), 893-919.

Joshi, A., Salaria, T., and Naidu, G., (2005), "India", in Campbell, D. (Ed.), E-commerce and the Law of Digital Signatures, Oceana, Dobbs Ferry, NY, pp. 289-327.

Kabanda, S., Tanner, M., and Kent, C., (2018), "Exploring SME cybersecurity practices in developing countries", Journal of Organizational Computing and Electronic Commerce, Vol. 28 No. 3,pp. 269-282.

Kasperky Lab 2013. Kaspersky Global IT Security Risks Survey 2013. Available: http://media.kaspersky.com/en/businesssecurity/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf. Last Accessed: 01/11/2019

Kaur, J.; Mustafa, N., (2013) "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," Research and Innovation in Information Systems (ICRIIS), International Conference on , vol., no., pp.286,290, 27-28 Nov. 2013.

Kendrick, R., (2010). Cyber Risks for Business Professionals: a Management Guide. Cambridgeshire: IT Governance Publishing

Kilic, M., and Uyar, A., (2017). Adoption process of IFRS for SMEs in Turkey: Insights from academics and accountants. Accounting and Management Information Systems, 16(2), 313-33

Khan, S. N., and Ali, E. I. E., (2017). The Moderating roel of intellectual ca[ital. between Enterprise Risk Management and Firm performance: A conceptual review. *American Journal of Social Sciences and Humanities*, 2(1), 9-15.

Kopia, J., Just, V., Geldmacher, W., and Bubian, A. (2017). Organization performance and enterprise risk management. Ecoforum, 6 (1)10.

Kraus, V., and Lehner, O. M., (2012). The nexus of Enterprise Risk Management and value creation: a systematic literature review. *ACRN Journal of Finance and Risk Perspectives*, 1(1), 92-163.

KPMG Risk report, (2018). 20 key risks to consider by Internal Audit before 2020. Website:
https://assets.kpmg/content/dam/kpmg/ch/pdf/key-risks-internal-audit-2018.pdf (Accessed 2 January 2020)

KPMG. "Small Business Reputation & the Cyber Risk.": n. pag. 2016. Web.
http://www.kpmg.com/channelislands/en/about/Documents/small-business-reputation-and-the-cyber-risk.pdf [Accessed on 10 December 2019]

Kwaramba, N. (2017). The role and importance of key entrepreneurship development. Retrieved from https://www.theindependent.co.zw/2017/05/26/role-importance-key-entrepreneurship-development/ (Accessed on 11 November 2019)

Liberto, D., (2019). Understanding Small and Mid-size Enterprise (SME). Small and Mid-size Enterprise (SME), pp. 12-25.

Macpherson, A., and Holt, R., (2007). Knowledge, learning and small firm growth – a systematic review of the evidence, Research Policy, 36: 172 – 192

Markowitz, H., (1952). Portfolio selection. *The Journal of Finance*, 7(1), 77-91.

Mayers, D., and Smith, C. W., (1987). Corporate Insurance and the Underinvestment Problem. *The Journal of Risk and Insurance*, 54(1) pp. 45-54.

McAfee (2014): Net Losses – Estimating the Global Cost of Cybercrime. http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf. Last accessed: January 16, 2019.

McShane, M.K., Nair, A., and Rustambekov, E. (2011). Does enterprise risk management increase firm value?. Journal of Accounting, Auditing & Finance, 26(4), 641-658.

Ministry of Information and Communication Technology (2015). Zimbabwe National Policy for Information and communication Technology (ICT) Draft. Harare: Government of Zimbabwe.

MISA-Zimbabwe. (2015). Internet Governance Multistakeholder Conference Report 2015: Supporting Free and Secure Online Expression and Access to Information in Zimbabwe. Harare: MISA-Zimbabwe.

Modigliani, M., and Miler, M., (1963). Corporate Income Taxes and the Cost of Capital: A Correction. *The American Economic Review, 53*(3), 433-443.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2013): Cyber-Risk Decision Models: To Insure IT or Not? Decision Support Systems 56(1), 11–26.

Mukhopadhyay, A., Saha, D., Mahanti, A. and Chakrabarti, B. B. (2005): Insurance for Cyber-Risk: A Utility Model, Decision 32(1), 153–169.
Naciye, S. (2015). Does Enterprise Risk Management Create value for firms? Evidence from Nordic Countries. Routledge Companion on Strategic Risk Management, Routledge

Natarajan, G. S and Wyrick, D. A (2011). Framework for implementing sustainable practices in SMEs in the United States, Proceedings of the World Congress on Engineering, 1: 40 – 71

National Association of Insurance Commissioners (NAIC) (2013), "Cyber risk", available at: www.naic.org/cipr_topics/topic_cyber_risk.htm (Accessed 4 January 2020).

Naude, M.J. and Chiweshe, N., 2017, 'A proposed operational risk management framework for small and medium enterprises', South African Journal of Economic and Management Sciences 20(1), 1–10. https://doi.org/10.4102/sajems.v20i1.1621

Nicholas, J. P. (2014, January 16). Cybersecurity Risk Paradox. http://blogs.microsoft.com/one-the-issues/2014/01/16/new-report-outlines-cybersecurity-challenges-in-developing-countries/ (Accessed 5 December 2019)

NIST (2018), "Framework for improving critical infrastructure cybersecurity version 1.1", available at: www.nist.gov/cyberframework (Accessed 23 November 2019).

Nocco, B. W. and Stulz, R. M (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance*, 18(4).

Norton Report (2013), Available: http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf. Last Accessed: 05/11/2019

Nurse, J.R.C., (2018), "Cybercrime and you: how criminals attack and the human factors that they seek to exploit", in Attrill-Smith, A., Fullwood, C., Keep, M. and Kuss, D.J. (Eds), The Oxford Handbook of Cyberpsychology, OUP, Oxford.

Nurse, J.R.C., Creese, S., Goldsmith, M., and Lamberts, K., (2011), "Trustworthy and effective communication of cybersecurity risks: a review", Workshop on Socio-Technical Aspects in Security and Trust, IEEE, pp. 60-68.

Nyathi, K.A., Nyoni, T., Nyoni, M and Bonga, W.G (2018). The Role of Accounting Information in the Success of Small & Medium Enterprises (SMEs) in Zimbabwe: A Case of Harare, Dynamic Research Journals Journal of Business and Management (DRJ – JBM), 1 (1): 01 – 15

Nyirenda-Jere, T., and Biru, T., (2015). Internet development and Internet governance in Africa. Internet Society.

OAS (2015), "Cybersecurity awareness campaign toolkit", available at: www.sites.oas.org/cyber/Documents/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20(English).pdf (Accessed 23 November 2019).

OECD. (2005). OECD SME and Entrepreneurship Outlook: 2005,. Paris: OECD.

OECD, 2009, Top barriers and drivers to SME internationalization, Report by OECD Working Party on SMEs and Entrepreneurship, OECD Publishing, viewed 01 January 2020, from https://strathprints.strath.ac.uk/15845/.

OECD/ IOPS (2011). Good Practices for Pension Funds' Risk Management Systems. *http://www.oecd.org/dataoecd/16/33/34018295.pdf.* Retrieved 25 October 2018.

Overby S., "Adopting ITIL, COBIT Is Not Always the Best Practice," CIO, February 2012, https://www.cio.com/article/2399188/it-organization/adopting-itil--cobit-is-not-always-the-best-practice.html

Ping A. T., and Muthuveloo, R., (2012). The Impact of Enterprise Risk Management on firm performance: Evidence from Malaysia. *Asian Social Science, 11(22),* 149-159.

Polkowski, Z., and Dysarz, J., (2017). It Security Management In Small And Medium Enterprises. Scientific Bulletin – Economic Sciences, Volume 16/ Special Issue EtaEc 2017, 2-16.

Quon, T.K., Zeghal, D. and Maingot, M. (2012). Enterprise Risk Management and firm performance. *Procedia-Social and Behavioral Sciences*, 62: 263-267.

Ramlee, R., and Ahmad, N., (2015). Panel Data Analysis on the Effect of Establishing the Enterprise Risk Management on Firms' Performance, Proceedings of 4th European Business Research Conference 9 - 10 April 2015, Imperial College, London

Reserve Bank of Zimbabwe. (2015). Cybercrime in Zimbabwe and Globally. Retrieved from RBZ Web site: www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf (Accessed on 19 November 2019)

Ridley, G., Young, J. and Carroll, P. 2004. COBIT and its utilization: A framework from the literature. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 5–8 January, 1–8, Big Island, Hawaii. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber =1265566 [Accessed 29 January 2020]

RSA Whitepaper (2016), Cyber Risk Appetite. Website: http://www.rsa.com/ (Accessed 14 December 2019)

Salzberg, C.A. and Jang, Y. (2012), "Policy initiative for health information technology: a qualitative study of US expectations and Canada's experience", International Journal of Medical Informatics, Vol. 81 No. 10, pp. 713-722.

Santos-Olmo, A., Sánchez, L.E., Caballero, O.I., Camacho, S. and Fernandez-Medina, E. (2016), "The importance of the security culture in SMEs as regards the correct management of the security of their assets", Future Internet, Vol. 8 No. 4, p. 30.

Saunders, M., Lewis, P., and Thornhill, A. (2012). *Research methods for Business Students.* 6th ed., Harlow, Pearson Education

Siam, W.Z., and Rahahleh, M.Y., (2010), Implications of applying the international financial reporting standards (IFRSs) for small and medium-sized enterprises on the accounting environment in Jordan, Journal of Accounting, Business and Management, Vol. 17, No. 2, pp 21-33

Sinanaj, G. and Muntermann, J. (2013), "Assessing corporate reputational damage of data breaches: an empirical analysis", Proceedings of the 26th International Bled eConference, Bled,pp.78-89.

Shuttleworth M., (2015). Internal Consistency Reliability. Viewed 21 January 2018, <https://explorable.com/internal-consistency-reliability>

Small Enterprise Development Corporation (SEDCO), 2011, Annual report. Entrepreneurship, 8(2010), viewed n.d., from www.sedco.co.zw

Smith, C. W., and Stulz, R. M. (1985). The Determinants of Firms Hedging Policies. *The Journal of Financial and Quantitative Analysis*, *20*(4), 391-405.

Swiss Re (2014): Working together with clients to find cyber risk solutions. http://www.swissre.com/reinsurance/insurers/casualty/smarter_together/working_smarter_together_for_cyberrisk_solutions_in_EMEA.html. Last accessed: December 18, 2019.

Szeman, P., (2005), "Hungary", in Campbell, D. (Ed.), E-commerce and the Law of Digital Signatures, Oceana, Dobbs Ferry, NY, pp. 269-285.

Tavakol M, Dennick R., (2011). Post-examination analysis of objective tests. Med Teach. 33:447-58

Taylor, M., and Murphy, A., (2004), "SMEs and eBusiness", Journal of Small Business and Enterprise Development, Vol. 11 No. 3, pp. 280-289.

Teoh A. P., and Muthuveloo, R., (2015). The Impact of Enterprise Risk Management on Firm Performance: Evidence from Malaysia, *Asian Social Science*, 11(22), 149-159.

Teoh, A. P., Lee, K. Y. and Muthuveloo, R. (2017). The Impact of Enterprise Risk Management, Strategic Agility, and Quality of Internal Audit Function on Firm Performance. *International Review of Management and Marketing, 7(1), 222-229.*

The Global Risks Report (2018). Website: https://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/ (Accessed on 2 December 2019)

Weston, J. F., and Copeland, T. E., (1998). Managerial Finance, CBS College Publishing, New York World Business Council for Sustainable Development [WBCSD] (2007). A business guide to development actors, WBCSD, Atar Roto, Switzerland

Uppal, S. M., Odhiambo, R. O., and Humphreys, H. M. (2005). Introduction to Probability and Statistics. JKUAT Press: ISBN 9966-923-95-0.

U.S. Department of Homeland Security (US DHS) (2018), "STOP. THINK. CONNECT campaign", available at: www.stopthinkconnect.org/ (Accessed 10 December 2019).

US State of Cybercrime Survey (2014), co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

Valli, C., Martinus, I.C. and Johnstone, M.N. (2014), "Small to medium enterprise cyber security awareness: an initial survey of Western Australian business", The International Conference on Security and Management, pp. 71-75.

Yang, S., Ishtiaq, M. and Anwar, M. (2018). Enterprise Risk Management Practices and Firm Performance, the Mediating Role of Competitive Advantage and the Moderating Role of Competitive

Advantage and the Moderating Role of Financial Literacy. *Journal of Risk Financial Management* 11 (35); doi: 10.3390/jrfm11030035

APPENDICES

UNIVERSITY OF ZIMBABWE

FACULTY OF COMMERCE

GRADUATE SCHOOL OF MANAGEMENT

Dear Respondent

RE: MBA RESEARCH QUESTIONAIRE

I am final year MBA student of the University of Zimbabwe carrying out a survey to investigate the impact of cyber risk management on the performance of Small and Medium Enterprises in Zimbabwe in partial fulfillment of the Masters of Business Administration Degree program. You have been selected to participate in this survey based on your position in the company structures. The findings of this study will be practically relevant to you and your company as it will aid you in building a resilient cyber risk management strategy in light of the turbulent macro-economic environment. A summary of the findings will be available at your request.

Please feel free and comfortable to complete the questionnaire as the responses to this survey completely anonymous and will be treated with utmost confidence. Therefore, it is important that you do not write your name or personal information on this copy.

Thank you in advance for taking your time to participate in this research study. This survey will take approximately 30 minutes of your time. The researcher can be contacted on 0772334151 or brighton.ganda@gmail.com if you need any clarifications.

Yours faithfully,

Brighton Ganda

SECTION A: GENERAL INFORMATION

This section contains 5 questions. Kindly show your response by ticking in the appropriate box.

1. Indicate the highest qualification that you have attained by the respondent.

   □ 'O" Level □ "A" Level □ Certificate/Diploma □ HND/Degree

   □ Post Graduate

2. How long have you been involved in company management?

   □ 0 - 1 year □ >1yr ≤ 5 years □ >5yr ≤ 10 years □ >10 years

3. Kindly select the option that best describes your role in your company governance structures?

   □ Owner □ Managing Director

   □ Finance Director □ Information Technology Manager

   □ Accountant □ Cyber Risk Manager

   □ Other (specify ……………………)

4. Tick an option that best describes the main economic activity of your enterprise?

Manufacturing		Wholesale and retail trade	
Electricity, gas, steam and air conditioning supply		Transportation and storage	
Financial and insurance activities			

5. Please indicate the number of employees in your company

1 – 20		21 – 40		41-60		61-80		81-100		100+	

6. Which option best describes the size of your company's annual revenue?

Less than $1000,000		$1000,001 – $2000,000		$2000,001- $3000,000		$3000,001- $4000,000		Above $4000,000	

7. In the last year, did your enterprise use any of the following digital technologies and/or applications?

Type of technology	**Tick the appropriate**
Broadband connection	
Website for your business	
Intranet (e.g. internal or private network)	
Enterprise resource planning (ERP) software package	
Customer relation management (CRM) software package	
Social media accounts (e.g. Facebook, Twitter, LinkedIn)	
E-commerce platforms and solutions (e.g. online payment and ordering)	
Cloud computing services	
Other (Please specify)	

SECTION B: MANAGEMENT OF RISKS

In the following segment you are asked to respond to statements concerning your opinions on how your company is managing strategic risks.

Please indicate your agreement to the statements using the following guidelines

1 = I strongly disagree with this statement
2 = I disagree with this statement
3 = Neutral
4 = I agree with this statement
5 = I strongly agree with this statement
Please tick or mark the rating that best describes your opinion on each statement

1. Cyber Risk management Governance	**Rating**				
	1	**2**	**3**	**4**	**5**
1.1. Our company's strategic plans are assessed for cyber risk that can impact on objectives.					
1.2. Cyber risk management is an integral part of our business strategy.					
1.3. The company employs a person primarily responsible for cyber risk management processes					
1.4. Governance structures are in place for deciding the acceptable level of cyber risk exposure to the business?					
1.5. The company reviews progress towards achievement of strategic plans on a regular basis?					
1.6. The company has structures or processes in place for reporting on cyber risk management to the Board and/or senior management?					

2. Cyber Risk Management Practices	**Rating**				
	1	**2**	**3**	**4**	**5**
2.1. Does your enterprise have a regular overall process to assess the risk to which its business activities are exposed?					
2.2. Cyber risk assessment is part of this overall risk assessment process?					

2.3. Regular assessment is carried out on the dependency of business activities on digital technologies and data					
2.4. Regular assessment is undertaken on the possibility of cyber risk incidents					
2.5. Regular assessment is done on the consequences of possible cyber risk incidents on business activities					
2.6. Employees are periodically trained on cyber risk assessment?					
2.7. Any cyber risk incidents are identified, thoroughly investigated and documented.					
2.8. Key cyber risk Indicators are clearly defined and periodically monitored.					

3. Cyber risk reduction practices	**Rating**				
	1	**2**	**3**	**4**	**5**
3.1. Information on cyber threats, vulnerability, incidents, risk management practice or security measures are communicated with other external stakeholders (e.g. industry players, customers, suppliers, police)?					
3.2. Cyber risk management measures in place aim to change the business activity (e.g. by redesigning or operating it differently)?					
3.3. Cyber risk information is available on timely basis to allow the Board of Directors to make informed decisions					
3.4. There is adequate communication to all key stakeholders of the adequacy of the cyber risk management system in place.					

4. Cyber risk management awareness and training	**Rating**				
	1	**2**	**3**	**4**	**5**
In the past year, the company performed the following:					
4.1. Referred to cyber risks in employment contracts					

4.2. Discussed cyber risks at business unit meetings					
4.3. Gave performance incentives to persons whose behaviour reduced cyber risk exposures					
4.4. Provided mandatory or optional training on managing cyber risk (e.g. online courses, workshops, seminars, conferences or training provided through internal meetings)					

SECTION C: IMPACT OF CYBER RISK

In the following segment, indicate your perception on the extent to which cyber risk has impacted on the performance of the company. indicate your agreement to the statements using the following guidelines

1 = No impact at all
2 = To a marginal extent
3 = To a moderate extent
4 = To a large extent
5 = To a very large extent

5. Impact Statement	**Rating**				
	1	**2**	**3**	**4**	**5**
5.1. Cyber risk has adversely impacted on the company's ability to achieves its strategic objectives					
5.2. Cyber risk has adversely impacted on the company's ability to make critical decisions					
5.3. Cyber risk has adversely impacted on the company's ability to grow over the last five years					
5.4. Cyber risk has adversely impacted on the company's ability to optimally allocate its resources					
5.5. Cyber risk has resulted with increased fraud and revenue pilferage cases					

SECTION D: PERFORMANCE MEASUREMENT

In the following segment, please provide responses to statements regarding the impact of cyber risk management practice on the performance of the company. Please indicate your agreement to the statements using the following guidelines

1 = I strongly disagree with this statement
2 = I disagree with this statement
3 = Neutral
4 = I agree with this statement
5 = I strongly agree with this statement

6. Performance measure	**Rating**				
	1	**2**	**3**	**4**	**5**
6.1. The company consistently achieves its strategic objectives					
6.2. Risk management has improved our decision making					
6.3. The company has achieved consistent growth over the last five years					
6.4. Allocation of resources has improved due to cyber risk management					
6.5. The stakeholders are satisfied with the company's performance.					
6.6. Fraud has reduced due to the adequacy of cyber risk management practises?					

The end

Thank you for your participation