Moderating role of entrepreneurial orientation on the relationship between information security management and firm performance in Kenya

Stanley Irungu Ndung'u

A Thesis Submitted in Partial Fulfilment for the Award of the Degree of Doctor of Philosophy in Entrepreneurship in the Jomo Kenyatta University of Agriculture and Technology

2014

DECLARATION

This thesis is my original work and has not been presented for a degree in any other university.

Signed ………………………………..… Date ……………………….

Stanley Irungu Ndung'u

This thesis has been submitted for examination with our approval as university supervisors.

Signed …………………................................... Date …………………….…

Dr. Robert Gichira

JKUAT, Kenya

Signed …………………................................... Date …………………….…

Prof. Waweru Mwangi

JKUAT, Kenya

Signed …………………................................... Date …………………….…

Dr. Kenneth L. Wanjau

Karatina University, Kenya

DEDICATION

To my wife Rachel, my daughters Faith and Peris, and my son, Joseph. It is through your patience, understanding, support and encouragement that I made it.

ACKNOWLEDGEMENT

It is only through enormous efforts that one is able to present a paper worth being referred to as a thesis. In the course of writing a thesis, one interacts with so many people, who in one way or the other assist in making it worthwhile. Thanks to all of you who made sure my thesis is a success. In particular, Dr. Robert Gichira, Prof. Waweru Mwangi and Dr. Kenneth Wanjau, my first, second and third supervisors respectively who, through their selfless effort, helped shape my ideas into a focused research area and ensured total success. It is through your wise counsel, guidance, encouragement and support that I made it. On the other hand, are my colleagues at work who, against all odds, assimilated most of my workload and thus enabled me to get enough time for my thesis.

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

COBRA	COst estimation, Benchmarking, and Risk Assessment
CORAS	Consultative Objective Risk Analysis System
CRAMM	(Central Computing and Telecommunications Agency – CCTA) Risk Analysis and Management Method)
CSI	Computer Security Institute
EU	European Union
FRAP	Facilitated Risk Analysis Process
ICT	Information and Communications Technology
IS	Information System
ISM	Information Security Management
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISRA	Information Security Risk Assessment
ISS	Information System Security
IT	Information Technology
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
OCTAVE-S	Operationally Critical Threat, Asset and Vulnerability Evaluation (for Smaller organisations)

PWC	PriceWaterhouseCoopers
ROE	Return on Equity
ROI	Return on Investment
ROS	Return on Sales
SME	Small and Medium Enterprises
UK	United Kingdom
USA	United States of America

DEFINITION OF TERMS

Cybercrime

Cyberspace crime (Gibson, 1984). Transformation of criminal or harmful behavior by networked technology (Wall, 2007). This study adopted the definition by Wall (2007).

Entrepreneurial Orientation

Entrepreneurial orientation is the extent to which a firm is entrepreneurial (Schillo, 2011). Entrepreneurial orientation also refers to the strategy making processes that provide organizations with a basis for entrepreneurial decisions and actions (e.g., Lumpkin & Dess, 1996; Wiklund & Shepherd, 2003). This study adopted Schillo (2011) definition.

Entrepreneurial Intensity

Entrepreneurial intensity is the degree and frequency of the practice of those activities characterized by their innovative, proactive and risk taking nature (Thoumrungroje, 2003). The varying levels of entrepreneurship are referred to as entrepreneurial intensity (Morris & Sexton, 1998). Entrepreneurship intensity also refers to the degree and frequency of entrepreneurship in the organization (Ireland, Kuratko, & Morris, 2006). This study adopted Thoumrungroje (2003) definition.

Firms

In this study, the term “firms” is taken in the same context as small and medium enterprises. Again, medium-sized firms especially in reference to Top 100 medium-sized firms, may in some instances be referred to as small and medium enterprises because their sizes in terms of number of employees employed fall within the parameters of small and medium enterprises.

Information Security

Information security is the protection of information within a business, and the systems and hardware used to store, process and transmit this information (Whitman & Mattord, 2005). Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Al-Awadi & Renaud, 2008). This study adopted the Whitman and Mattord (2005) definition of information security.

Information Security Breach

Term used to describe failure to protect sensitive and confidential information and information systems from unauthorized access, use, or disclosure (Berezina, Cobanoglu, Miller & Kwansa, 2012). Information security breach is a situation where an individual intentionally exceeds or misuses network, system, or data access in a manner that negatively affects the security of the organization's data, systems, or operations (Kassner, 2009). This study adopted Berezina et al (2012) definition of information security breach.

Information Security Risk Assessment (ISRA)

Information security risk assessment (ISRA) is a systematic method by which organizations can identify and protect information assets to achieve a desired level of security (Lichtenstein, 1996). Information security risk assessment is the process of assigning risk ratings or scores to each specific information asset based on their threats and vulnerabilities (Whitman & Mattord, 2003). This study adopted the Lichtenstein (1996) definition of Information security risk assessment.

Information Technology

Those technologies engaged in the operation, collection, transport, retrieving, storage, access, presentation and transformation of information in all its forms (Dhillon, 2007). Wide range of computerized information and communication technologies including products and services such as desktop computers, laptops, hand-held devices, wired and wireless intranet, business productivity software such as text editor and spreadsheet, enterprise software, data storage and security, network security and others (Ashrafi & Murtaza, 2008). This study adopted Dhillon (2007) definition.

Information Security Management (ISM)

Information security management is a series of management activities with the aim of protecting and securing information assets within the framework of the organization in which information system is running (Kazemi et al, 2012). Information security management is a part of contingency management that is meant for the prevention, detection and reaction to the threats, vulnerabilities and impacts inside and outside of an organization (Robbins, 1994). This study adopted Kazemi et al. (2012) definition of Information security management.

Small and Medium Enterprises (SMEs)

These are enterprises comprising of 10 to 100 workers (Gray, 2000). Enterprises having fewer than 10 employees and a turnover not exceeding €2 million are categorized as "micro", those with fewer than 50 employees and a turnover not exceeding €10 million as "small", and those with fewer than 250 and a turnover not exceeding €50 million as "medium" (European Commission, 2013). The European Commission (2013) definition prevailed in this study. The terms “small business” and SME are sometimes used interchangeably since SMEs share many of the characteristics of their smaller counterparts (Schaper & Volery, 2004).

Strategic Entrepreneurship

This is a process that facilitates firm efforts to identify opportunities with the highest potential to lead to value creation, through the entrepreneurial component and then to exploit them through measured strategic actions, based on their resource base (Kyrgidou & Hughes, 2010). Strategic entrepreneurship also refers to capitalizing on both opportunity-seeking activities which inherently characterize entrepreneurship, as well as advantage-seeking activities demanded by strategy (Ketchen, Ireland & Snow, 2007). This study adopted Kyrgidou and Hughes (2010) definition.

Technology Entrepreneurship

Ways in which entrepreneurs draw on resources and structures to exploit emerging technology opportunities (Liu et al., 2005). Also defined as the transformation of promising technologies into value (Petti & Zhang, 2011). This study adopted Petti and Zhang (2011) definition.

ABSTRACT

The purpose of this study was to investigate the moderating role of entrepreneurial orientation (EO) on the relationship between information security management (ISM) and firm performance in Kenya. Research has shown that in an environment of dynamic technology and shortened product and business model lifecycles, firms may benefit from adopting both an EO and strategic entrepreneurship in their quest for sustained competitive advantage. Technological advances contribute to market imperfections, in turn leading to the formation of entrepreneurial opportunities, a demonstration that technological entrepreneurship transforms promising technologies into value. However, increasing dependence on technology by organizations to drive businesses and to create a competitive advantage makes ISM for organizations extremely challenging. Companies suffer significant financial and reputational damage due to ineffective ISM, severely impacting firm's performance and their market valuation. This study tested the null hypotheses that top management commitment, information security policy enforcement, human-related information security issues, IT competence, and information security risk assessment have no relationship with firm performance in Kenya and the null hypothesis that, EO does not moderate the influence of ISM on firm performance in Kenya. Positivism paradigm approach and mixed method research guided by cross-sectional survey design was adopted in this study. The target population for this study were the medium-sized companies in Kenya, and the respondents were the IT managers of these firms. The study used a census approach. A self-administered, semi-structured questionnaire was used to collect primary data. Secondary data was obtained from published sources such as library, internet and research done by other scholars. The questionnaire was tested for validity and reliability. Quantitative and qualitative techniques were used to analyze the collected data with the assistance of Statistical Package for Social Sciences (SPSS) software, Ms-Excel, Analysis of Moment Structures (AMOS), SmartPLS, STATA, R-GUI and ATLAS.ti software. Analyses were conducted using a two-phase process consisting of confirmatory measurement model and confirmatory structural model. Also, moderated multiple regression (MMR) analysis was carried out by comparing ordinary least-squares (OLS) regression model and MMR model. The study found that top management commitment, human-related information security issues and information security risk assessment were individually significant predictors of firm performance with information security risk assessment being the most significant predictor of the three. The results also revealed that EO significantly moderated the relationship between information security management and firm performance. Overall, the study demonstrated positive relationship between technological entrepreneurship and firm performance. This study recommends that factors associated with technology need to be enhanced by including them in the mission and vision statements of firms and making them part of their code of conduct as they have the greatest impact on firm performance. EO concept should be made a management philosophy in majority of firms, and finally, firms should be encouraged to increase their entrepreneurial intensity levels for superior performance. Lastly, effective implementation of ISM is capable of creating greater gaps between the leaders and laggards in the market, thus creating a pattern that closely matches the turbulent “creative destruction” mode of capitalism known as “Schumpeterian competition”.

CHAPTER ONE

INTRODUCTION

1.1 Overview

This chapter reviews the background of the study, statement of the problem, objectives of the study, research hypothesis, justification, significance, and scope of the study. The last section in the chapter covers the limitations of the study.

1.2 Background of the Study

In an environment of rapid change (dynamic technology) and shortened product and business model lifecycles, the future profit streams from existing operations are uncertain and businesses need to constantly seek out new opportunities (Rauch, Wiklund, Lumpkin & Frese, 2009). Therefore, firms may benefit from adopting an entrepreneurial orientation in their quest for sustained competitive advantage. Such firms innovate repeatedly while taking risks in their product market strategies. Efforts to anticipate demand and aggressively position new product/service offerings often result in strong performance (Ireland, Hitt, & Sirmon, 2003). Thus, conceptual arguments suggest that entrepreneurial orientation leads to higher performance and can also drive a firm to enhance business performance and competitiveness.

However, Morris and Sexton (1996) regard entrepreneurial orientation as a one-dimensional view of the entrepreneurship phenomenon. Therefore, another dimension, namely frequency of entrepreneurship was included, and the phenomenon named entrepreneurial intensity, a function of the degree and frequency of entrepreneurship (Heilbrunn, 2008). Since Entrepreneurial intensity is positively related with firm's financial and non-financial performance (Dong, 2009), increased entrepreneurial intensity levels, therefore, can only lead to superior firm performance.

Strategic entrepreneurship (SE) is also gaining increasing interest chiefly in established businesses that strive to develop a more entrepreneurial orientation (EO) in their pursuit for continuous competitive advantage (Schiendel & Hitt, 2007). Strategic entrepreneurship involves the integration of two disciplines, that is, those of entrepreneurship and strategic management. The former consists of actions for and behaviors contributing to identifying and exploiting profitable opportunities in the environment, and the latter involves the set of actions designed to achieve competitive advantage and achieve better-than-average results by intelligent and fact-based selection among alternatives leading to such advantage (Shane & Venkataraman, 2000).

There is now wide-spread agreement that changes in technology (technological advances) are among the key sources that contribute to the market imperfections which lead to the formation of entrepreneurial opportunities (Petti & Zhang, 2011). Literature has demonstrated the positive relationship between technological advances and firm profitability (Cefis & Ciccarelli, 2005). The key challenge for enterprises is rather how to best exploit and transform the promising technologies into new products and processes, because technologies are only more likely to contribute to value creation when they are successfully commercialized, and only when the capabilities to successfully commercialize those technologies are heterogeneously distributed across firms, Gans and Stern (2003) as cited in (Petti and Zhang, 2011).

However, the ever-growing dependence of organizations on technology to drive businesses and to create a competitive advantage makes information security management for organizations extremely challenging (Onwubiko & Lenaghan, 2009). The development of information and communication technology (ICT) and the spread of the Internet are remarkably changing individual lifestyles and business conduct and also explosively creating new businesses (Park, Jang & Park, 2010). But at the same time, adverse changes and effects such as hacking, viruses and personal information leaking are also rapidly increasing. Therefore, it has become a key task for governments, enterprises and individuals reliant on the Internet to effectively cope with problems of information security. Chiefly, enterprises corresponding to a backbone of a modern society recognize information security management as one of business management factors (Park, Jang & Park, 2010).

Information security management is categorized as the preservation of confidentiality, integrity and availability (Chang & Ho, 2006). Chang and Ho further explains that confidentiality is ensuring that information is accessible only to those authorized to have access; integrity is the safeguarding of the accuracy and completeness of information and processing methods; and availability is ensuring that authorized users have access to information and associated assets when required. Chang & Ho further aver that information security management protects information, including trade secrets, from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments. Companies suffer significant financial and reputational damage due to ineffective information security management, which has comprehensively been shown to severely affect firms' performance and their market valuation (Gupta, 2011). Global economic losses due to information security breaches is estimated to be over $1trillion (Mills, 2009), and the average data breach event in the United States costs an organization USD 8.9 million (Saad, 2013). In Kenya, two thirds of businesses and other organizations are victims of economic crime (Global Economic Crime Survey, 2011).

Despite the availability of numerous methods and publications on how organizations can manage information security risks, small and medium enterprises still face serious challenges in managing cybercrime and resulting losses (Bougaardt and Kyobe, 2011). Almost 90% of the small and medium enterprises globally are victims of data theft or data loss in some form or the other (Karimpanal, 2012). Many organizations would like to have a secure information technology environment, but very often this need comes into conflict with other urgencies. Small and medium enterprises particularly face a range of factors and obstacles including unfamiliarity with information security management issues, more pressing needs, tight constraints on money and resources, and a craving to ignore anything that is not directly involved with business survival and growth (Lacey & James, 2010).

However, small and medium enterprises should consistently focus on threats that are likely to have an impact on, and affect the organization (Lacey & James, 2010). Moreover, small and medium enterprises require a range of security advice and solutions, from simple tips on relatively low cost policy and awareness measures to more sophisticated, technology solutions that require specialist external advice. Accordingly, this calls for more investment in Information Technology resources. A research by McAfee and Brynjolfsson (2008) discovered that changes in competitive dynamics were most ostensible in precisely those sectors that had spent more on information technology.

To better understand when and where information technology confers competitive advantage in today’s economy, McAfee and Brynjolfsson (2008) studied all publicly traded United States companies in all industries from the 1960s through 2005, looking at pertinent performance indicators from each including sales, earnings, profitability, and market capitalization. They found some salient patterns: since the mid-1990s (which marked the mainstream adoption of the internet and commercial enterprise software), a new competitive dynamic had emerged - greater gaps between the leaders and laggards in an industry, more concentrated and winner-take-all markets, and more churn among rivals in a sector. Amazingly, this pattern closely matched the turbulent “creative destruction” mode of capitalism (Schumpeter, 1942).

The need to link information security management with performance has become especially important for firms striving to achieve superior firm performance (Bose, Luo & Liu, 2013). However, there have been little documented evidences that existed for specific relationships between information security management and performance. Thus, the relationship remains blurred. Also, there is no rich literature available that directly investigate the moderating role of entrepreneurial orientation on the relationship between information security management and firm's performance. Specifically, the impact of information security management on performance is expected to depend on firm's entrepreneurial orientation. This was the rationale for conducting this research. Overall, the study advanced technology entrepreneurship anchored on Schumpeterian competition, or more specifically, the theory of creative destruction.

1.2.1 Global Perspective of Information Security Management

Due to lack of adequate security practices and infrastructure, targeted attacks are growing the most among businesses with fewer than 250 employees (Symantec, 2013). Small businesses are now the target of 31 percent of all attacks, a threefold increase from 2011, with the cybercriminals using small firms as a conduit to ultimately reach larger companies. Web-based attacks increased by 30 percent in 2012, many of which originated from the compromised websites of small firms (Symantec, 2013).

It is estimated that about 85 percent of all United States of America companies have experienced one or more information security breaches (Riddell, 2011). The average cost of a data breach for a firm is $7.2 million, an increase of seven percent from the year before, and lost business represented 63 percent of the total cost in the United States (Ponemon, 2010). The average data breach event in the United States costs an organization $8.9 million (Saad, 2013).

In the United Kingdom, one in seven large organizations has detected hackers within their systems - the highest level ever recorded since the survey started in the early 1990s (Porter, 2012). Additionally, 70% of large organizations have detected significant attempts to break into their networks in the last year, while 15% of them had their networks successfully penetrated by hackers. The average cost of a large organization’s worst security breach of the year is £110,000-£250,000 and £15,000-£30,000 for a small and medium enterprise (Porter, 2012).

In Australia, 60% of small business owners have suffered a security breach, with losses of up to $20,000 reported by 47% of respondents (Bourke, 2011). A further 10.1% had suffered losses of $20,000 to $100,000 and 3% had dealt with losses of more than $100,000. Despite this, small and medium enterprises do not rate security as a critical factor in the running of a business, with one third of the owners stating that investing money in security is not important to them. Bourke further reported that as many as 73% of small business owners confessed to possessing only average to low security knowledge levels. In India, only 15% of small and medium firms could claim that their data was secure (Karimpanal, 2012).

Global economic losses due to information security breaches in 2008 amounted to over $1trillion (Mills, 2009). From a global perspective, almost 90% of the small and medium firms are victims of data theft or data loss in some form or the other (Karimpanal, 2012).

1.2.2 Kenyan Perspective of Information Security Management

Statistics from Communication Commission of Kenya indicates that by the end of 2011, over 36 per cent of the population had access to Internet from 31.8 per cent recorded in 2010 (Olingo, 2012). This means that the rapid growth in Internet penetration is exposing more Kenyans to risk. Two thirds of businesses and other organizations in Kenya are victims of economic crime (Global Economic Crime Survey, 2011). The survey revealed that cybercrime, at 22%, now ranks as one of the top four economic crimes in Kenya, among Africa respondents and globally, after asset misappropriation (73%), accounting fraud (38%) and bribery and corruption (23%). In total, 66% of respondents in Kenya said their organizations were victims of economic crime, nearly double the global average of 34% and a 9% point increase since 2009. Kenya recorded the highest level of economic crime among all 78 countries surveyed. It was ranked second highest in 2009 behind South Africa.

A global Internet security report covering security of small and medium-sized firms' bank account information, customer data and intellectual property, positions Kenya at number eight in Africa in terms of threat, a reflection of the wide usage of the Internet by companies (Symantec, 2013). The report further indicates that Kenya only improved slightly moving to position 86 globally in 2012 from the previous 85 in 2011 in terms of security threat level. Lack of adequate security practices and infrastructure among the small and medium-sized firms has provided a fertile ground for cyber criminals who are having a field day mining confidential data from the gullible businesses.

1.2.3 Top 100 Small and Medium Enterprises in Kenya

Kenya’s Top 100 Survey is an initiative of KPMG Kenya and Nation Media Group. The Survey seeks to identify Kenya’s fastest growing small and medium-sized firms in order to showcase business excellence and highlight some of the country’s most successful entrepreneurship stories. The important role that these companies play in economic growth has often gone unappreciated especially because little is said about the number of direct and indirect jobs that they create and the amount they pay in taxes, which may not be much if looked at separately, but which is significant if they are pooled (Mureithi, 2013).

One of the challenges facing the country today has been that its import bill perennially exceeds income from exports (BD, 2012). But if the small and medium-sized firms are nurtured and encouraged to export more of their products, they have the potential of helping the country address the imbalance between imports and exports. BD further states that these small and medium-sized firms can also help Kenya achieve the broad goals outlined in Vision 2030 of making the country industrialized and with a high quality of life for its citizens. The companies can also be showcased as potential avenues for job creation, especially among the youthful population. The Top 100 Survey recognizes the fastest growing medium-sized companies with annual turnovers of between Sh70 million and Sh1 billion. The sector accounts for 60 per cent of the country's labor market and has an estimated combined annual turnover of nearly Sh100 billion or 10 per cent of the country's Budget (BD, 2012).

1.3 Statement of the Problem

In Kenya, the Top 100 medium-sized companies have an estimated combined annual turnover of nearly Sh100 billion or 10 per cent of the country's budget, and the sector accounts for 60% of the country's labor market (Juma, 2011). However, small and medium enterprises (SMEs) still face serious challenges in managing cybercrime and resulting losses (Bougaardt & Kyobe, 2011). Top 100 medium-sized firms, and SMEs in general, have the potential to contribute more positively to the Kenyan economy than is currently the case. But to survive in a turbulent and dynamic business environment, they have to formulate and implement their strategy by engaging in entrepreneurial behaviors.

Despite the availability of numerous methods and publications on how organizations can manage information security risks, many SMEs fail to identify or recognize and account for losses and continue to ignore the implementation of effective information security measures (Kyobe, 2008).

That is why Kenya only improved slightly moving to position 86 globally from the previous 85 in 2011 in terms of security threat level (Symantec, 2013). This is likely to lead to sure death of small and medium enterprises, in turn lowering of the country's gross domestic product (GDP). Increasing negative gross domestic product stirs worry of economic recession in economists and investors.

One prominent concept of strategy-making in entrepreneurship literature is entrepreneurial orientation (EO) (Schiendel & Hitt, 2007). Therefore it is expected that adopting entrepreneurial orientation may enhance the information security management (ISM)-firm performance relationship in SMEs in Kenya, particularly given their resource limitations.

Several studies have been done on the area of ISM. Kimwele (2012) studied on Information Technology security in SMEs, Ogalo (2012) studied on the impact of information system security policies and controls on firm operation enhancement for Kenyan SMEs, Global Economic Crime Survey (2011) reported on the general economic crime in Kenya and Kimwele, Mwangi and Kimani (2011) studied on information technology security management in Kenyan SMEs. This shows that limited attention has been paid to the moderating role of EO on ISM-firm performance relationship model. This study filled in on this existing knowledge gap.

1.4 Objectives of the Study

1.4.1 General Objective

The main objective of this study was to investigate the moderating role of entrepreneurial orientation on the relationship between information security management and firm performance in Kenya.

1.4.2 Specific Objectives

1. To investigate the influence of top management commitment on firm performance in Kenya.
2. To establish the influence of information security policy enforcement on firm performance in Kenya.
3. To explore the effect of human-related information security issues (culture, awareness and training) on firm performance in Kenya.
4. To assess the influence of information technology competence on firm performance in Kenya.
5. To determine the effect of information security risk assessment on firm performance in Kenya.
6. To determine whether entrepreneurial orientation moderates the relationship between information security management and firm performance in Kenya.

1.5 Research Hypothesis

To examine how each of the independent variables influences the response variable, this study tested the following null hypotheses:

H_{01}: There is no relationship between top management commitment and firm performance.

H_{02}: There is no relationship between information security policy and firm performance.

H_{03}: There is no relationship between human-related information security issues and firm performance.

H_{04}: There is no relationship between information technology competence and firm performance.

H_{05}: There is no relationship between information security risk assessment and firm performance.

H_{06}: Entrepreneurial orientation does not moderate the relationship between information security management and firm performance.

1.6 Justification of the Study

Nowadays, small and medium enterprises are increasingly considered as the main part of modern economy, important participants in innovative activities in economy and a source of competition, job creation and human resource flexibility. This is because they constitute over 90% of businesses worldwide and nearly 50% of total world employment (Moor & Manring, 2009). This study focused on the top 100 medium-sized companies in Kenya. These enterprises are Kenya’s fastest growing and if well nurtured have the potential of helping the country address the imbalance between imports and exports, cognizant of the fact that Kenya’s import bill perennially exceeds income from exports. Also, they can help Kenya achieve the broad goals outlined in Vision 2030 of making Kenya industrialized. The important role that these companies play in economic growth has often gone unappreciated especially because little is said about the number of direct and indirect jobs that they create and the amount they pay in taxes, which may not be much if looked at individually but which is significant if they are pooled (Mureithi, 2013). The sector accounts for 60 per cent of the country's labor market and has an estimated combined annual turnover of nearly Sh100 billion or 10 per cent of the country's Budget (BD, 2012).

On the other hand, research shows that companies suffer significant financial and reputational damage due to ineffective information security management, severely impacting firm's performance and their market valuation (Gupta, 2011). Chang and Ho (2006) posit that information security management protects information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments. Even though there are now a few interesting and growing, albeit slowly, number of studies addressing factors that determine effective implementation of information security management within the specific context of small and medium enterprises, there is no rich literature available in developing countries, Kenya included, in relation to information security management as a major factor to the overall performance and success of small and medium enterprises.

1.7 Significance of the Study

This study benefits the small and medium enterprises owners / managers realize the potential benefits of information security management. They will also realize that information security is indeed not an Information Technology problem, but a business problem. It is therefore their responsibility to take a lead in driving effective information security practices and ensuring that the organization is well protected from cyber-attacks. Academic researchers will be able to refer to the data used in the study and benefit from the findings, cognizant of the fact that rich literature is unavailable in Kenya relating information security management to firm performance. The industry will benefit from the novel knowledge in the study. Lastly, the findings of the study will provide the insights to the Government policy makers as it will show whether information security management affects performance of small and medium enterprises. Based on the findings, the policy makers will come up with the way forward on how to revitalize the firms.

1.8 Scope of the Study

This study embarked on 2013 Top 100 medium-sized firms in Kenya. These firms contribute significantly to the Kenyan economy. They have a workforce of between 10 to 250 employees, have an estimated combined annual turnover of nearly Sh100 billion, and the sector accounts for 60% of the country's labor market. The sub-variables of entrepreneurial orientation are the commonly studied ones (Kroon, Voorde and Timmers, 2013; Lisboa, Skarmeas and Lages, 2011; Hughes and Morgan, 2007; Wiklund and Shepherd, 2003; Miller, 1983). However, they have not been tested in this kind of relationship. Information security management has a mixture of sub-variables that are commonly studied (non-technical factors) and others that are hardly studied (technical ones). For the latter, the study wished to interrogate them more to add knowledge on technological and strategic entrepreneurship, while with the former, the study wished to test the sub-variables in this kind of relationship because they have hardly been tested in it before. The sub-variables of firm performance were chosen because it is easy for small and medium enterprises to use them to measure their performance (Liang, You & Liu, 2010). The period of study was 3 months.

1.9 Limitations of the Study

The idea of information security is sensitive and not easy. This study explored the opinions of Information Technology managers regarding typical activities with security implications within their firms. Therefore, the effect of the small size of the sample might be a decreased generalizability of the findings. However, this was mitigated against by carrying out the bootstrapping procedure. The study used ordinal scale among others to measure the variables. However, ordinal scale does not give the investigator the level of precision required in a study, especially when strong statistical procedures are to be applied (Mugenda, 2008). Also, because the respondent is the sole data source for both independent and dependent variables, common method variance could introduce spurious correlation between the variables (Avolio, Yammarino & Bass, 1991; Jap & Anderson, 2004). However, a test of common method variance resulted in a value that was within the acceptable thresholds, thus mitigating against the limitation.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter covers the strategic entrepreneurship concept, information security management concept, theoretical and empirical literature that is relevant to the area of study. A conceptual framework is also developed. This is followed by critique of the existing literature, research gaps and summary of the empirical literature.

2.1.1 Entrepreneurial Orientation Concept

The extent to which a firm is entrepreneurial is commonly referred to as its entrepreneurial orientation (Schillo, 2011). Entrepreneurial orientation should be seen as a process reflected in recurring organizational behavior (Covin & Slevin 1991) rather than the actions of individuals possessing certain attributes or characteristics. There is widespread agreement amongst researchers that entrepreneurial orientation has three core dimensions: innovativeness, proactiveness and risk-taking (Kroon, Voorde and Timmers, 2013; Lisboa, Skarmeas and Lages, 2011; Hughes and Morgan, 2007; Wiklund and Shepherd, 2003; Miller, 1983). This is because in some studies, competitive aggressiveness and proactiveness have been treated as the same (Antoncic and Hisrich, 2003; Morris, 1994).

Innovativeness is the firm’s ability and willingness to support creativity, new ideas and experimentation which may result in new products/services (Lumpkin & Dess, 1996), while proactiveness is the pursuit of opportunities and competitive rivalry in anticipation of future demand to create change and shape the business environment (Lumpkin & Dess, 2001). Relating to risk-taking, it is the firm knowingly devoting resources to projects with chance of high returns but may also entail a possibility of high failure (Lumpkin & Dess, 1996). However, risk-taking is also commonly associated with entrepreneurial behavior and that generally successful entrepreneurs are risk-takers (Hodgetts & Kuratko, 2001). Miller (1983) argued that these three components of EO comprised a basic unidimensional strategic orientation.

2.1.2 Information Security Management Concept

Given the integral role of Information Technology in today’s firms, information security has to be a key component in modern enterprise planning and management. This entrenchment of information security was also driven by the increasing growth of electronic transactions and fueled partly by the Internet as electronic commerce thrived with the growth of networks. As enterprise boundaries become faint, security at the enterprise level becomes more challenging (Chang & Ho, 2006). Chang and Ho aver that information security management protects information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments. These threats are, *inter alia*, computer-assisted fraud, sabotage, vandalism, theft, fire or flood, and damages caused by breaches such as computer viruses and computer hacking.

While the attacks of computer systems or misuse of these systems had been slowly and steadily decreasing over years, both the average reported annual loss per firm and the average reported loss per incidence were not decreasing (Chang & Lin, 2007). This is mainly due to the fact that organizations have focused their computer security practice largely on technical issues like access controls, forgetting that economic, financial and risk management aspects of computer security have become more and more important concerns to today's organizations, and such concerns are complements to, rather than substitute for, the technical aspects of computer security. Kazemi, Khajouei and Nasrabadi (2012) explain that the scope of information security includes the protection of all verbal and print information, and information that are automatically recorded for the use by people in organizations. The scope also includes the protection of all resources that are used for creating, processing, transmitting, storing, using, viewing or controlling the facilities of restricted environments, communication networks, information staff, peripheral devices, storage and recorded media.

2.1.3 Technological Entrepreneurship Concept

Technologies create value when they are transformed into new products, the new products rapidly introduced to the market and extra-profits for enterprises, appropriate returns for investors, rewards for inventors and ultimately benefits for the whole society are generated (Petti & Zhang, 2011). That is, technological entrepreneurship is the transformation of promising technologies into value. More specifically, technological entrepreneurship consists of a set of behaviors and actions that drive the market process (and also a strategy) which is based on identifying high potential, technology-intensive commercial opportunities, gathering/assembling resource and managing rapid growth and significant risk with the final aim to exploit those opportunities for value creation (Cefis & Ciccarelli, 2005).

In this regard, technological entrepreneurship concept is made of an entrepreneurial component, that is, the enterprise's capabilities to recognize technologies' entrepreneurial and business opportunities, and a management component, that is, the enterprise's capabilities to develop compelling value propositions and business models made to exploit those opportunities (Bingham, Eisenhardt & Furr, 2007). These two capabilities make technological entrepreneurship capabilities, that is, the capabilities to identify and exploit technological opportunities to create new or significantly improved products and to successfully commercialize them. There is also an environmental component to consider, that is, the availability and the qualities of external institutions and resources that set the appropriate conditions for technological opportunities to be discovered and exploited profitably (Petti & Zhang, 2011).

2.2 Theoretical Literature

A theory is a set of systematic interrelated concepts, definitions and propositions that are advanced to explain and predict phenomena (Cooper & Schindler, 2011). This section covers the theories that are relevant in explaining the moderating role of entrepreneurial orientation on the relationship between information security management on performance of firms.

2.2.1 Creative Destruction Theory

This theory proposes that companies holding monopolies based on incumbent technologies have less incentive to innovate than potential rivals, and therefore they eventually lose their technological leadership role when new radical technological innovations are adopted by new firms which are ready to take the risks (Foster & Kaplan, 2001). Foster and Kaplan further emphasize that when the radical innovations eventually become the new technological paradigm, the beginner companies leapfrog ahead of former leading firms.

Schumpeter (1942) posits that innovation causes market dislocations, which allow the ascendance of new firms and the corresponding decline of the large incumbent firms whose leadership positions they assume. This occurs through the introduction of: the new commodity, the new technology, the new source of supply, the new type of organization - competition which commands a decisive cost or quality advantage and which strikes not at the margins of the profits and the output of the existing firms but at their foundations and their very lives.

This theory is important to this study in more ways than one. In the late 20th century, traditional industries in the United States of America with higher firm-specific stock returns and fundamental performance heterogeneity used Information Technology (IT) more intensively to post faster productivity growth (Chun, Kim, Morck & Yeung, 2007). It can be argued that this mechanically reflects a wave of Schumpeter’s (1942) creative destruction disrupting a wide swath of industries, with successful Information Technology adopters unpredictably undermining established firms.

This was further confirmed by McAfee and Brynjolfsson (2008) who discovered that the changes in competitive dynamics in the United States companies were most apparent in those sectors that had spent the most on information technology. This is a pattern that closely matches the turbulent “creative destruction” mode of capitalism. Consequently, this study is anchored on the creative destruction theory.

However, society cannot reap the rewards of creative destruction without accepting that some individuals might be worse off, not just in the short term, but perhaps forever. At the same time, attempts to soften the harsher aspects of creative destruction by trying to preserve jobs or protect industries will lead to stagnation and decline, short-circuiting the march of progress. Schumpeter’s enduring term is a reminder that capitalism’s pain and gain are intricately linked. The process of creating new industries does not go forward without sweeping away the preexisting order (Richard & Kaplan, 2001).

2.2.2 Diffusion of Innovations Theory

The diffusion of innovations theory centers on the conditions which increase or decrease the likelihood that a new idea, product, or practice will be adopted by members of a given culture.

Diffusion of innovations theory predicts that media as well as interpersonal contacts provide information and influence opinion and judgment. Studying how innovation occurs, Rogers (1995) argued that it consists of four stages: invention, diffusion (or communication) through the social system, time and consequences. The information flows through networks. The nature of networks and the roles opinion leaders play in them determine the likelihood that the innovation will be adopted. Innovation diffusion research attempts to explain the variables influencing how and why users adopt a new information medium, such as the Internet, with opinion leaders' personal contact exerting influence on audience behavior.

Five adopter categories are: (1) innovators, (2) early adopters, (3) early majority, (4) late majority, and (5) laggards. These categories follow a standard deviation-curve: very little innovators adopt the innovation in the beginning (2.5%), early adopters making up for 13.5% a short time later, the early majority 34%, the late majority 34% and after some time finally the laggards make up for 16% (See Figure 2.1).

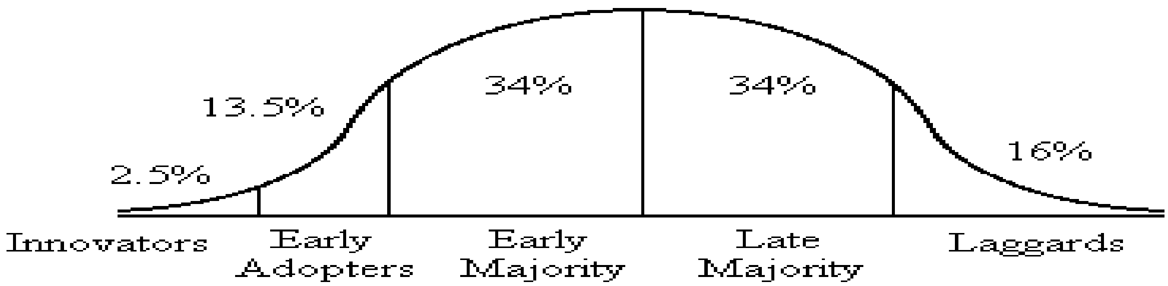


Figure 2.1 Hypothesized distribution of adopter categories within a typical population (Rogers, 1995).

There are five main factors that influence adoption of an innovation, and each of these factors is at play to a different extent in the five adopter categories. These are; Relative Advantage (the degree to which an innovation is seen as better than the idea, program, or product it replaces); Compatibility (how consistent the innovation is with the values, experiences, and needs of the potential adopters); Complexity (how difficult the innovation is to understand and/or use); Triability (the extent to which the innovation can be tested or experimented with before a commitment to adopt is made); and Observability (the extent to which the innovation provides tangible results) (Rogers, 1995).

This theory is useful in this study since research shows that firms seeking to be competitive and responsive to environmental changes introduce innovations (Uzkurt, Kumar, Kimzan, & Eminoglu, 2013). The same research emphasizes that mechanisms should be sought to encourage and foster an innovative culture in organizations since these are likely to facilitate the introduction, adoption and diffusion of innovations which, in turn, is likely to result in achievement of superior firm performance.

2.2.3 Deterrence Theory

Information security policy and information security training are vital parts for maximizing information systems security (Rezgui and Marks, 2008). However, employees not adhering to security policies and not practicing what they learned in training can lead to unintentional mistakes and financial losses for organizations (CSI, 2010). Proponents of Deterrence Theory believe that people will engage in criminal or deviant behavior if they do not fear apprehension and punishment (Keel, 2005). Keel states that Deterrence theory has two major uses, that is, specific deterrence and general deterrence. Specific deterrence is focused on punishing known deviants to keep them from again violating specific norms of society. General deterrence is focused on reducing deviance in the general population by focusing on future behaviors. People in society are deterred from deviant activities because of their fear of punishment and that fear is reinforced by their knowledge of others getting punished. Deterrence Theory's shaming is a technique for encouraging employees to adhere more to information security policies and training (Harris, 2012).

In this study, this theory shows the importance of information security policy and information security training in maximizing information systems security leading to overall firm performance. Anticipated shaming is also important as a method of encouraging employees to follow information security policies and training. However, the shaming technique requires the individual to have a respectful relationship with peers because if an employee does not respect coworkers, shaming might not work because the employee might not care enough about what coworkers think about their relationship. To get the best results from the shaming technique, management should consider building better relationships among employees for the shaming technique to have a better chance of working. This translates to incurring expenditure to fund social events for employees.

2.2.4 Risk Management Theory

Risk management theory suggests that through organizational risk analysis and evaluation, the threats and vulnerabilities regarding information security could be estimated and assessed (Hong, Chi, Chao & Tang, 2003). The evaluation results could be used for planning information security requirements and risk control measures, with the ultimate goal of reducing or minimizing information security risk to an acceptable level in an organization.

Wright (1999) revealed that risk management is a process of establishing and maintaining information security inside an organization. Wright posits that the crux of risk management is risk assessment. In other words, through information security risk assessment, a firm could take appropriate measures to protect information cost-effectively. The interaction of risk assessment and risk control minimizes information security risk to an acceptable level and actualizes the control procedures. The relationships could thus be expressed in the following way: information security = *f* (risk assessment, risk control, review and modification); risk assessment = *f* (risk analysis, risk estimation); risk control = *f* (establishment of control measures, implementation); risk analysis = *f* (threats, vulnerability); and risk estimate = *f* (impact, asset appraisal).

This theory is important in this study since it understands and copes with insecure environments. However, the theory ignores security policy and information audit mechanisms and overemphasizes on structures. This study explored the relationship between information security policy and firm performance.

2.2.5 Neo-institutional Theory

Neo-institutional theory explains how external influences cause organizations to become similar over time through the process of isomorphism, isomorphism being a factor in assimilation of enterprise resource planning systems (DiMaggio & Powell, 1983). Neo-institutional theory has been used in information system (IS) research (Liang, Saraf, Hu & Xue, 2007) and information system security (ISS) research (Hu, Hart & Cooke, 2007) and is used here to examine normative (changes that result from professionalization of the workforce), mimetic (which occur when organizations copy practices from other organizations they perceive as successful, and are common in uncertain environments), and coercive (external influences from regulatory sources, competition, and society that pressure organizations to change) mechanisms that drive isomorphism (DiMaggio & Powell, 1983) and affect information system security assimilation in organizations. Hu, Hart and Cooke (2007) explain that mimetic, normative and coercive mechanisms are important factors in the adoption of inter-organizational information system and in particular, coercive and mimetic mechanisms are important to the establishment and effectiveness of information system security programs.

Management research shows senior management selects strategic organizational issues (Dutton & Ashford, 1993), which can come from either external or internal sources. Senior management is the primary human agent between external influences and organizational change (Liang, Saraf, Hu & Xue, 2007), and external influences motivate senior management to commit to information system security thus improving information system security in organizations. Figure 2.2 illustrates the Neo-institutional theory framework.

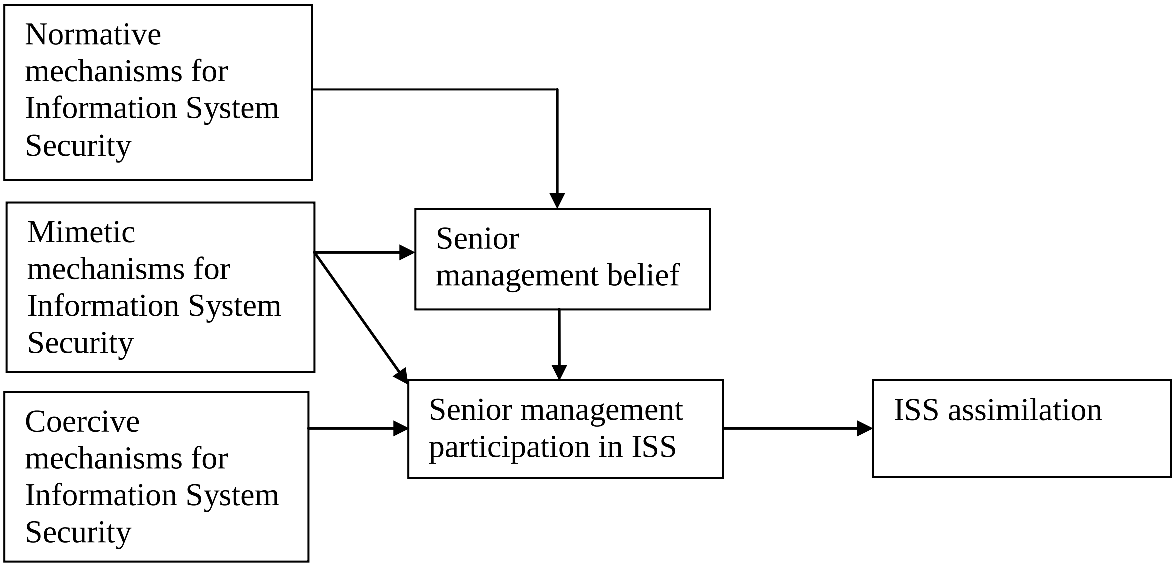

Normative mechanisms for Information System Security
Mimetic mechanisms for Information System Security
Coercive mechanisms for Information System Security
Senior management belief
Senior management participation in ISS
ISS assimilation

Figure 2.2 Neo-institutional theory framework (Tejay & Barton, 2013)

As shown in figure 2.2, senior management belief in information system security and senior management participation in information system security are mediating constructs between external influences and information system security assimilation. Senior management belief in information system security also influences senior management participation in information system security (Liang, Saraf, Hu & Xue, 2007). Mimetic mechanisms influence senior management belief, and directly influence senior management participation. Normative mechanisms directly influence senior management belief, and senior management participation in information system security is evidenced by their actions to establish authority and responsibilities, communicate a vision, manage, lead, and align information system security with organizational strategy. In short, external influences motivate senior management to commit to information system security (McFadzean, Ezingeard & Birchall, 2011).

This theory is important to this study because it was used to examine normative, mimetic, and coercive mechanisms that affect ISS assimilation in organizations. In short, it demonstrates how external influences motivate senior management to commit to information system security. However, low levels of normative influences were reported in the study of the theory, yet high levels of senior management belief in information system security were similarly reported. This suggests managers receive minimal education on information system security through industry channels, yet they will still have developed an awareness of information system security. This is a contradiction requiring broader studies.

2.3 Conceptual Framework

A conceptual framework is a model of presentation where a researcher conceptualizes or represents the relationships between variables in the study and shows the relationship graphically or diagrammatically (Orodho, 2008). In this context, Orodho posits, a conceptual framework is a hypothesized model identifying the concepts or variables under study and showing their relationships. Kothari (2009) defines a variable as a concept that can take different quantitative value such as weight, height, or income. Mugenda (2008), on the other hand, defines a variable as a measurable characteristic that assumes different values among units of specific population.

The key variables in this study were categorized as independent variable, moderator and dependent variable. Mugenda (2008) explains that the independent variables are called predictor variables because they predict the amount of variation that occurs in another variable while dependent variable, also called criterion variable, is a variable that is influenced or changed by another variable. The dependent variable is the variable that the researcher wishes to explain. A moderator variable is a variable that alters the strength of the causal relationship (Frazier, Tix, & Barron, 2004).

This study analyzed how top management commitment, information security policy enforcement, human-related information security issues (culture, awareness and training), information technology competence, and information security risk assessment influence firm performance. This relationship was moderated by entrepreneurial orientation. The variables in the conceptual framework were derived from the theories identified in this study. The variables were also derived from the studies done by the following scholars: (Kazemi, Khajouei & Nasrabadi, 2012; Babatunde & Selamat, 2012; Kimwele, Mwangi & Kimani, 2011; Al-Awadi & Renaud, 2008; Chang & Ho, 2006; Knapp, 2005; Johnson, 2005; Upfold & Sewry, 2006; Rastogi, 2011, Shedden, Scheepers, Smith & Ahmad, 2011; Braber, Hogganvik, Lund, Stolen & Vrallsen, 2007; Dhillon, 2005; Pattinson & Anderson, 2007).

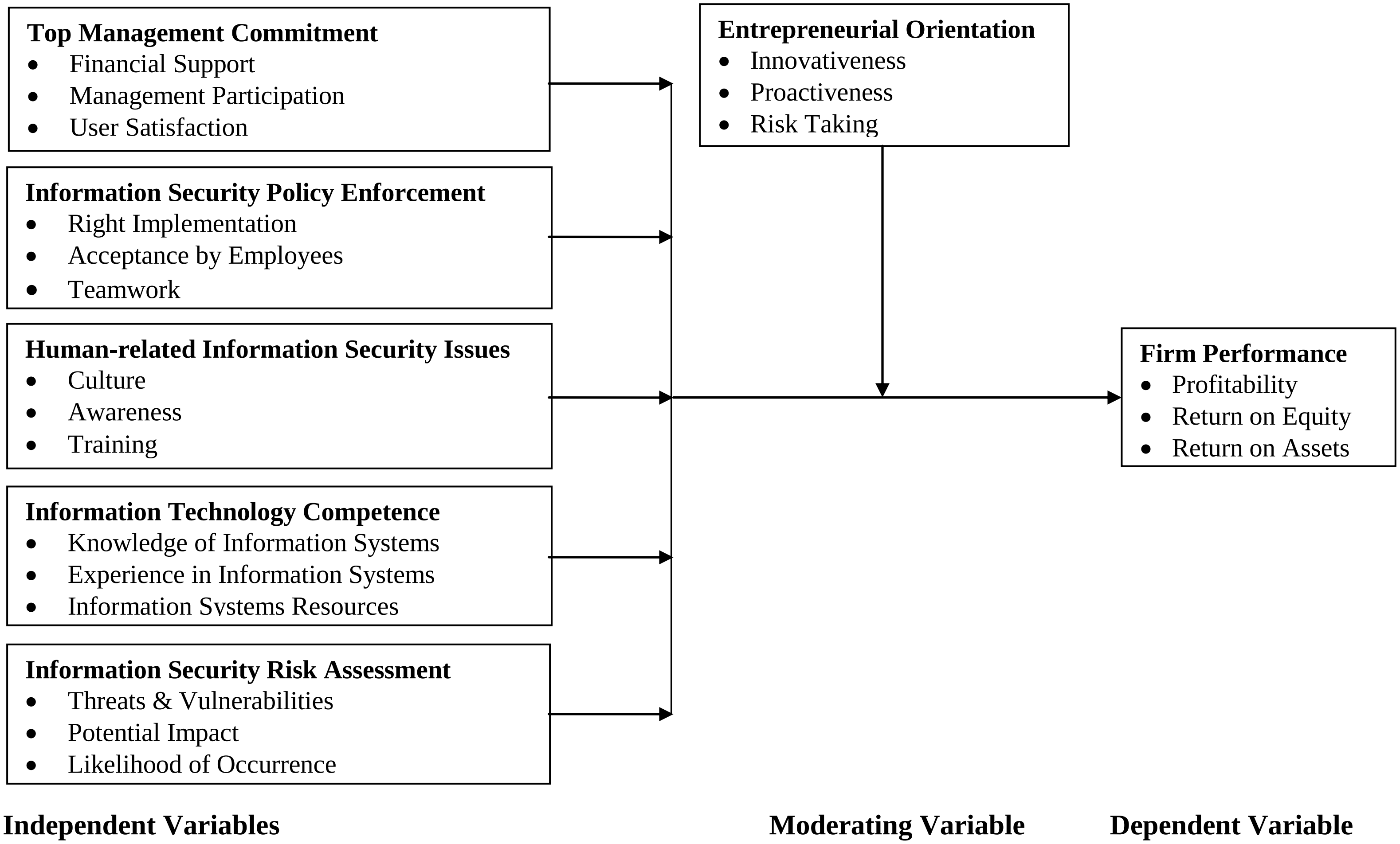


Figure 2.3 Conceptual Framework

2.3.1 Top Management Commitment

Great scholars on information systems underscore the importance of the top management commitment as a success factor for managing information security, and influencing the employees below them (Liang et al, 2007). Thus, top management commitment and participation in information security initiatives gives an impression of their support and other employees will not see the initiatives as an extra burden but a signal of how to value the initiatives. Liang et al posit that user satisfaction represents the success of various managerial interventions designed to promote end-user adoption. Indeed, if the top management do not support or understand the need of information security the implementation of information security will fail (Al-Awadi & Renaud, 2008). One of the objectives of the study was to investigate the effect of top management commitment on firm performance in Kenya. Therefore the following hypothesis was proposed:

H_{01}: There is no relationship between top management commitment and firm performance in Kenya.

2.3.2 Information Security Policy Enforcement

Information security policy is important because it is the main tool for achievement in information security management activities (Kazemi, Khajouei & Nasrabadi, 2012). The performance of an organization will be successful if when a policy is created it is rightly implemented, accepted by employees, and the rules followed without manipulating them (Al-

Awadi, 2009). Enforcement of the information security policy is by putting it into practice because this ensures that employees can follow the rules and know their rights and responsibilities (Kazemi, Khajouei & Nasrabadi, 2012). They further opine that policy effectiveness is relevant to everyone's job in the organization because everyone is affected by information security to some extent; thus teamwork is encouraged. From the foregoing discussion, therefore, the following hypothesis was tested:

H_{02}: There is no relationship between information security policy enforcement and firm performance in Kenya.

2.3.3 Human-related Information Security Issues

Information security culture is embedded in organization culture, the backbone of efficient business value, which guides and enables employees to be committed to the organization. It acts like a guide to shape the employees behavior in order to fulfill organizational mission and vision (Babatunde & Selamat, 2012). Furthermore, information security culture is an approved method in which employees' duties are carried out in the organization. Therefore, the impact of information security culture on the aspect of improving performance, information policy and managerial effectiveness cannot be over emphasized.

To help employees practice information security properly and reduce the number of errors they make, organizations need to apply training and awareness programs (Al-Awadi, 2009). Al-

Awadi opines that training and awareness programs will enhance the implementation of information security and make the implementation of security easier. As a result when an organization institutes awareness programs employees change their behavior from being security vulnerable to a more defensive element against security breaches; organizations should therefore not underestimate the importance of information security awareness and training (Kazemi et al., 2012). Therefore the following hypothesis was tested:

H_{03}: There is no relationship between human-related information security issues and firm performance in Kenya.

2.3.4 Information Technology Competence

Information Technology competence can be defined as the set of Information Technology-related knowledge and experience that a business manager possesses (Bassellier, Reich & Benbasat, 2001). Information Technology competence enables a company to plan, organize, execute, and invest on information security effectively (Chang & Ho, 2006). Technological competencies consist of knowledge and skills embedded in people and intangibles embedded in technical system (Bassellier et al., 2001). Alshawaf, Ali and Hassan (2005), on the other hand, found that managers' knowledge of Information Systems, together with Information Systems resources, was a key factor affecting information security management. From this discussion, the following hypothesis was proposed:

H_{04}: There is no relationship between information technology competence and firm performance in Kenya.

2.3.5 Information Security Risk Assessment

Risks to assets are identified in terms of confidentiality, integrity and availability (Shedden, Scheepers, Smith & Ahmad, 2011), and the criticality of each risk is rated according to potential impact and likelihood of occurrence. There are a number of popular Information Security Risk Assessment methodologies in global use in the industries including FRAP, CRAMM, COBRA, OCTAVE, OCTAVE-S and CORAS (Dhillon, 2007), and although they differ in their make-up, order and depth of activities, they generally follow a three-stage pattern: context establishment, risk identification, and risk analysis. Dhillon explains that context establishment stage allows for the scoping and focus of the rest of the risk assessment process for maximum effectiveness and to ensure that any risks inherent in the organization's industry or line of business are identified. Risk identification concerns the identification of the threats and vulnerabilities of each of the most critical assets. Risk analysis concerns the determination of probability and impact (the cost of compromising the asset). The integration of the probability and impact will present the level of risk. Therefore, the following hypothesis was proposed:

H_{05}: There is no relationship between information security risk assessment and firm performance in Kenya.

2.3.6 Entrepreneurial Orientation and Firm Performance

Entrepreneurial orientation (EO) results in the destruction of old business practice stereotypes and the establishment of new, innovative, risk-tolerating patterns of economic behavior (Huang, Wang, Chen, & Yien, 2011) and there is also reason to believe that entrepreneurial orientation can have positive performance implications that are universal. Indeed, entrepreneurial orientation is a significant contributor to a firm's success. Entrepreneurial orientation has a positive impact on firm performance and several empirical studies find support for that view (Covin & Slevin, 1991; Lumpkin & Dess, 1996; Wiklund, 1999), an indication that entrepreneurial orientation plays an important role in organizational success and leads to better firm performance (Huang, Wang, Chen & Yien, 2011). Studies have found positive effect of entrepreneurial orientation on growth of small firms (Hughes and Morgan, 2007; Lumpkin and Dess, 1996). Proactive firms seek specific and valuable resources to enhance their competitive advantage (Hughes & Morgan, 2007). Moreover, to introduce new products and services, innovative firms are more than likely to explore unique resources and new possibilities to undermine their competitors (Huang, Lee & Kao, 2006). Therefore the following hypothesis was tested:

H_{06}: Entrepreneurial orientation does not moderate the influence of information security management on firm performance in Kenya.

2.3.7 Moderating Role of Entrepreneurial Orientation on the Relationship between Information Security Management and Firm Performance

Information security management has a great impact on firm's performance (Bose et al., 2013), and entrepreneurial orientation might improve the information security management. Specifically, the impact of information security management on performance depends on firms' entrepreneurial orientation. In the literature, there are only a few researchers who have discussed directly on the relationship between information security management and entrepreneurial orientation. Most of studies investigated the context of Knowledge-based Resources with entrepreneurial orientation (Wiklund & Shepherd, 2003); Cultural Diversity with entrepreneurial orientation (Richard, Barnett, Dwyer & Chadwick, 2004); Organizational culture with entrepreneurial orientation (Lumpkin & Dess, 1996; Chadwick, Barnett & Dwyer, 2001); Top management team characteristics with entrepreneurial orientation (Lumpkin & Dess, 1996).

Organizational culture, in which information security culture is embedded, is a key determinant of a firm's ability to understand, develop, or maintain entrepreneurial activity (Richard et al., 2004). Overall, organizational culture can be the factor that sends an organization to greatness as its members are inspired to do their utmost to work hard to conceive and make goods and services that improve the welfare of their customers and hence develop organizational competences and obtain a competitive advantage. Chadwick et al (2001) agree with this and state that a positive culture would be one that supports risk-taking, opportunity seeking, and innovation. This illustrates that culture is a determinant of entrepreneurial orientation.

With the context of top management commitment with entrepreneurial orientation, Hambrick and Mason (1984) suggested that top management characteristics do not occur in isolation, but rather are significantly traceable to the top-most manager. They further suggest that the top-most manager as leader nearly dominates group characteristics. Hence, it stands to reason that top managers influence entrepreneurial orientation and other firm characteristics (Ireland, Covin, & Kuratko, 2009) by encouraging their organizations in general, and top management team members in particular, to be more responsive and committed to initiating and supporting innovative entrepreneurial initiatives. In this context, it can be assumed that entrepreneurial orientation will moderate the relationship between information security management and performance.

2.3.8 Firm Performance

Performance improvement is the primary goal of all entrepreneurial firms as it demonstrates the level of success of its business operations (Wang, 2008). Various firm performance measurements have been applied in previous studies. However, the majority of these studies did not provide any justification for the selection of measures used, and there has not been any agreement among entrepreneurship scholars on the assignment of an appropriate set of measurements (Madsen, 2007).

To capture different aspects of firm performance, multiple measures, that is, financial and non-financial should be employed. However, most studies apply only financial measurement to assess performance, with firm performance being investigated as the dependent variable (Wang, 2008). The three dimensions used in the financial measurement are efficiency, growth and profit. Liang, You and Liu (2010) on the other hand state that firm performance refers to organizational effectiveness in terms of its financial and operational performance, and a number of indicators are used to measure it, including finance, efficiency, customer satisfaction, value addition, and market share. Liang et al further posit that financial indicators include commonly used measures such as Return on Investment (ROI) or the measure of profitability for a given amount of time, Return on Equity (ROE), Return on Sales (ROS), Return on Assets (ROA) revenue, and sale. These indicators usually can show the firm's capability in making profits. Efficiency-related indicators are productivity and cost reduction.

Lastly, firm performance can be assessed objectively as well as subjectively. The former relies on secondary or accounting data and the latter is based on respondents' perceptions or self-reported data. While objective measurement has an advantage in reducing common method variance, it is often difficult to accomplish (Stam & Elfring, 2008). The alternative is subjective measurement, which is conducted by comparing a firm's current performance with its previous performance (Wang, 2008). This study adopted subjective measurement.

2.4 Empirical Literature

Ko and Dorantes (2006) investigated the impact of information security breaches on financial performance of the breached firms. They considered subsequent four quarters following the security breach and determine if the breached firms' (treatment firms) performance decreased compared to that of the peer firms (control group). They found out that although the breached firms' sales and operating income did not decrease in the subsequent quarters following the breach, return on assets decreased in the third quarter. Also, performance of the control firms was higher compared to that of the treatment firms in general. However, the breached firms' sales increased significantly in the fourth quarter compared to those of the control firms, suggesting that information security breaches have minimal long-term economic impact. One possible explanation is that the breached firms responded to the breach incident by making additional security investment to prevent from any future breaches and the other explanation being that as the time passes, people forget about what happened earlier and the impact of the breach on financial performance phases out over the long-term.

Hall, Sarkani and Mazzuchi (2011) carried out a study to examine the relationship between information security strategy and organization performance. Findings suggested that organizational capabilities, encompassing the ability to develop high-quality situational awareness of the current and future threat environment, the ability to possess appropriate means, and the ability to orchestrate the means to respond to information security threats, were positively associated with effective implementation of information security strategy, which in turn positively affects organization performance. The study findings yield practical value for business leaders in understanding the viable predisposition of organizational capabilities in the context of information security, thus enabling firms to focus on acquiring the ones indispensable for improving organization performance.

Berezina, Cobanoglu, Miller and Kwansa, (2012) investigated the impact of information security breaches on hotel guests' perceived service quality, satisfaction, likelihood of recommending a hotel and revisit intentions. The results of the study revealed a significant impact of the treatments on three of the four outcome variables: satisfaction, likelihood of recommending a hotel, and revisit intentions. Information security breach scenarios resulted in a negative impact on the outcome variables regardless of whether or not the guest's credit card information was compromised. In other words, identity theft undermines hotel credibility with respect to perceived service quality and customers' trust. Above that, overall satisfaction, revisit intentions and likelihood of recommending a hotel to others were also negatively affected by the information security breach. A positive scenario though, revealed a significant increase in guest satisfaction and revisit intentions scores. In turn, this would lead to better performance by the hotel. This study contributes to the body of knowledge on the importance of credit card information security breaches to hotel guest satisfaction and future behavior.

Bougaardt and Kyobe (2011) investigated the factors that inhibit small and medium enterprises from recognizing and measuring losses from cyber-attacks in South Africa. The investigations revealed three major problems. The first problem was lack of awareness and understanding of what cyber-attacks involve, resulting in the continued victimization of these firms. The second one was an apparent limited effort to ensure accurate and reliable data for the purpose of analysis even in those organizations that claimed to have up-to-date software, hardware and anti-virus programs, and the third problem was that the employees were still unaware of the requirements of the Electronic Communications and Transactions (ECT) Act and penalties, despite their organizations claiming to recognize and prepare loss estimates. Recommendations were provided on how SMEs can address this problem, including creating awareness through training on cyber-attacks, training in record-keeping practices and use of readily available (on-line) statistics on crime, attacks and vulnerabilities.

In their study on financial impact of information security breaches on breached firms and their non-breached competitors, in which they focused on specific types of information security breaches: denial of service, website defacement, data theft, and data corruption, Zafar, Ko & Osei-Bryson (2012) found statistically significant evidence of the presence of intra-industry information transfer for some types of security breaches, suggesting that a security breach announcement is not just an incident to the breached firm but it has a ripple effect to the industry as a whole. They also found evidence of contagion effects (meaning that an information security breach incident is also viewed as bad news to its competitors in the same industry and thus, both the breached firm and its competitor firms strive to improve their overall company image and industry image as a whole) but no similar evidence concerning competition effect.

Cavusoglu, Mishra and Raghunathan (2004) studied the effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. They found that that announcing an Internet security breach is negatively associated with the market value of the announcing firm. They also found out that the effects of security breaches are not restricted to the breached firms, because the market value of security developers is positively associated with the disclosure of security breaches by other firms. The security developers in the sample realized an average abnormal return of 1.36 percent during the two-day period after the announcement - an average gain of $1.06 billion in two days. The study suggests that the cost of poor security is very high for investors.

Gordon, Loeb and Zhou (2011) studied the impact of information security breaches: has there been a downward shift in costs? They came up with three major findings. The first was that the impact of the broad class of information security breaches on stock market returns of firms was significant. The second was that when breaches were classified by their primary effect in terms of confidentiality, availability or integrity, attacks associated with breaches of availability had the greatest negative effect on stock market returns. The third was that there was a significant downward shift in the impact of the security breaches in the sub-period following the 9/11/2001 attacks versus the impact in the pre-9/11 period.

Kimwele, Mwangi and Kimani (2011) studied on Information Technology security management in Kenyan small and medium enterprises. They looked at whether SMEs have a designated employee in charge of IT security, whether SMEs seek external expertise about IT security where it is not internally available, if employees are aware that IT security incidents should be reported to management immediately, whether SMEs have a formal disciplinary process for employees who violate the company's IT security policies and processes and if their IT security measures have been reviewed within the last year. The study revealed that Kenyan SMEs do not have in place proper IT security management practices. The survey also revealed that SMEs need to put in place good management and disciplinary measures if they are to realize the benefits of IT security.

The study on an investigation of information security in small and medium enterprises (SME's) in the Eastern Cape by Upfold and Sewry (2005) revealed that the level of information security awareness amongst SME leadership is as diverse as the state of practice of their information systems and technology. Although a minority of SME's do embrace security frameworks such as SABS ISO/IEC 17799 or the International equivalent, BS7799, most SME leaders have not heard of security standards, and see information security as a technical intervention designed to address virus threats and data backups. And despite several "stripped-down" standards and guidelines available for SME's and based mostly on SABS ISO/IEC 17799 but designed as streamlined, they are scarcely used and are largely unknown by SME's.

2.5 Critique of the Existing Literature

Ko and Dorantes (2006) conducted a research on the impact of information security breaches on financial performance of the breached firms. This study was conducted using the "matched sample comparison group" method although using a case study approach would have offered additional insights about the differences between the groups. The study also included only 19 security breaches involving confidential data. Apart from limiting the generalizability of the results by the small sample size, more current security breach events and different types of events to evaluate the impact of security breach by type would have been more suitable. Also, accounting measures may not be the best measure to evaluate the impact of security breaches although they are the most commonly used financial performance measure in the previous studies.

The study by Hall et al (2011) to examine the relationship between information security strategy and organization performance may be characterized by a potential source of bias resulting from the technical nature of the intended population. The study primarily polled information security specialists and there may be a chance the results could have been partially influenced by their inherently technical perspective. Thus the targeted sample should have exemplified a reasonable mix of information security professionals and individuals in managerial and strategic planning positions in order to realize greater generalizability of the results. Also to further the generalized knowledge of the impacts of organizational capabilities in information security, incorporating a higher percentage of senior managers and executives in the respondent sample is worth exploring.

The study by Berezina et al (2012) on impact of information security on hotel guests' perception of service quality, overall satisfaction, revisit intentions and likelihood of recommending a hotel to others, had some limitations. The use of an online instrument for data collection meant that only persons with valid e-mail addresses could be recruited for the study, thus affecting the generalizability of the findings. The sample is heavily represented by females and leisure travelers leading to a small proportion of participants, whereas one would have preferred a sample that is more evenly distributed. Also, in spite of this study implementing PERFQUAL instrument to test if the information security breach/no-breach scenarios will shift customers perceptions and intentions overall, a specific measurement scale may be proposed for the information technology quality to provide a more precise picture for hoteliers and researchers working in the field of hotel information technology.

Due to the small sample size (22 SMEs) and the number of items used to measure the constructs, the quality of IS design and awareness and compliance with regulations did not have significant influence on recognition and measuring losses in the study by Bougaardt and Kyobe (2011) which investigated the factors that inhibit SMEs from recognizing and measuring losses from cyber-attacks in South Africa. If repeated with a much larger sample and the relationships between the constructs tested again in a regression analysis, the findings would be worth generalizing. The limited size also made it impossible for the study to compare the responses of business managers and IT/IS staff, which could in turn reveal more details about the potential causes of different behaviors of managers towards security. Future studies should investigate these relationships and their impact on the dependent variable.

The study by Zafar, Ko & Osei-Bryson (2012) only considered publicly traded firms. Efforts should have been made to gather financial performance data of private firms too. Although their study considered the industry average to compute the expected performance as a whole over a period of an entire year, it may however, also be argued that events other than information security breaches (e.g. change in executive management) may have been responsible for the change in performance. Also, for each breached firm they matched its financial performance against the average financial performance of its multiple competitor firms. However, given the possibility that some of the breached firm's competitors may have experienced contagion effects while others experienced competition effects, then it is possible that these two types of effects could have canceled each other out in the calculation of the average performance of the breached firm's competitors.

The study by Cavusoglu, Mishra and Raghunathan (2004) used event-study methodology, which assumes that markets are efficient and investors are rational, to estimate the cost of security breach events for firms. Thus, their study, like all other event studies, suffers from the fact that real markets can deviate from such an ideal characterization. The time period used for the study was characterized by high market valuation and market volatility, and while this by itself does not invalidate the event-study methodology, it indeed may increase the errors in the estimates of breach cost. An effort was made to eliminate all known confounding events from the sample, but this was not enough since other unknown factors that may affect a firm's market valuation during the event window may increase the error in the estimates of breach cost. The study also focused on publicly traded United States of America firms. This in itself limits the generalization of the results to other countries. Categorization of breach types in the study resulted in a primitive classification whereas a finer classification would require more sample data to have sufficient statistical power. Further research could provide additional insights into the impact of breach type on capital markets.

Gordon, Loeb and Zhou (2011) study employed event-study methodology. First, if the market is not fundamentally efficient, the event-study formulation would not be expected to capture the economic impacts of information security breaches and a completely different methodology for examining the economic impact of security breaches would have to be used. Also, since the study only examined the security breaches that were reported in major publications, the methodology tends to limit the analysis to breaches affecting larger firms.

Kimwele, Mwangi and Kimani (2011) study randomly identified one hundred and twelve (112) SMEs to participate in the survey, out of which twenty one (21) completed questionnaires were collected. The respondents included business decision makers, IT managers, or people who take care of computers systems in SMEs. The data on exact number of respondents in terms of nature of business, length of time the business has been in operation, current number of employees, number of computers used in the businesses and how long they have used computers were collected. The small sample size (21) limited the generalizability of the results. Future studies should relate management of information technology to the performance of SMEs.

The study by Upfold and Sewry (2005) used a survey questionnaire to collect data from 32 SMEs out the total 37. While the response rate was impressive at 86.5%, the sample size was still too small to generalize the results. Still, SME's must formalize information security by adopting a security standard. Part of the difficulty for SME's wishing to implement a universal standard such as ISO/IEC 17799, is that the standard is complex and all embracing, while SME's typically do not have the resources to embark on drawn-out implementations.

2.6 Summary of the Literature Review

This chapter has covered the theoretical framework, conceptual framework, empirical review and the literature gaps. The theoretical framework has provided a theoretical understanding of the research by reviewing theories related to the study. The literature has affirmed that companies suffer significant financial and reputational damage due to ineffective information security management, which has extensively been shown to severely impact firm's performance and their market valuation.

Empirical studies have also shown that despite the availability of numerous methods and publications on how organizations can manage information security risks, small and medium enterprises still face serious challenges in managing cybercrime and the resulting losses. Consequently, their risk exposure to cyber-attacks and the resulting losses continue to rise. But that information security management protects information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments. The moderating role of entrepreneurial orientation to improve on the causal effect of information security management on firm performance has also been introduced. This study reviewed this in details since not much has been done in this area.

2.6 Research Gaps

Several studies have tested the moderating role of entrepreneurship orientation, including Lumpkin and Sloat (2001) in their study on do family firms have an entrepreneurial orientation?; Wiklund and Shepherd (2003) in their study on knowledge-based resources, entrepreneurial orientation and the performance of small and medium-sized business; and Richard, Barnett, Dwyer and Chadwick (2004) in their study on cultural diversity in management, firm performance, and the moderating role of entrepreneurial orientation dimensions. But none has so far been tested on the role of entrepreneurship orientation on the relationship between information security management and firm performance.

Moreover, the few studies that have been done on the area of information security management mostly in Europe, Asia and the United States of America fail to relate information security management on firm performance. Dhillon (2007) studied on the principles of information systems security; Gupta (2011) studied on three essays on information technology security management in organizations; Berezina et al (2011) investigated the impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth; Eloff and Eloff (2003) studied on information security management as a new paradigm; Huang et al (2006) studied on balancing performance measures for information security management; Kazemi et al (2012) based their study on an evaluation of information security management system success factors.

Others are Huang et al (2006) in their study on balancing performance measures for information security management; Park et al (2010) in their study on effect of information security management system certification on organization performance; Rastogi (2011) in the study on information security service management - a service management approach to information security management; Upfold and Sewry (2005) in their study on an investigation of information security in small and medium enterprises in the Eastern Cape; and Carey-Smith (2011) on improving information security management in nonprofit organizations.

Yet only a few studies have been carried out in Kenya including Kimwele et al (2011) on their study on information technology security management in Kenyan small and medium enterprises;

Kimwele (2012) on information technology security in small and medium enterprises; and Ogalo (2012) in his study on the impact of information system security policies and controls on firm operation enhancement for Kenyan small and medium enterprises. These studies show that limited attention has been paid to the moderating role of EO on ISM-firm performance relationship model in Kenya. This study therefore filled in on this existing knowledge gap. The study also added value to existing literature by providing empirical information security management measures that small and medium enterprises in Kenya can take in order to improve on their performance.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the research design and the methodology that was used in this study. It starts with the research philosophy. The philosophy is followed by research design, population, sampling size and sampling technique, data collection instruments, data collection procedure, pilot study, measurement and scaling technique, data analysis and processing, and statistical model and hypothesis testing.

3.2 Research Design

This study was a mixed methods research guided by cross-sectional survey design. Research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in the procedure (Orodho, 2008); thus, Orodho asserts, decisions regarding what, where, when, how much, by what means concerning an inquiry or research study constitutes a research design. Research design constitutes the blue print for collection, measurement and analysis of the data (Cooper & Schindler, 2011; Kothari, 2009). Cooper and Schindler (2011) posit that research design enables the researcher in allocation of limited resources by posing crucial choices in methodology. Kothari (2009), on the other hand, clarify that the design includes an outline of what the researcher will do from writing hypothesis and its operational implications to the final analysis of data.

Mixed methods research allows a researcher to combine elements of qualitative and quantitative research approaches (Johnson, Onwuegbuzie & Turner, 2007). The use of mixed methods research allows the researcher to compensate for the weakness of one single approach with the strengths of the other in order to achieve the best results (Cresswell & Clark, 2011). Kusumawardhani (2013) in her study on The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java, used mixed methods research.

Cross-sectional survey design, on the other hand, helps with hypothesis formulation and testing the analysis of the relationship between variables (Kothari, 2004). Therefore this design was appropriate for this study which extensively tested the analysis of the relationships between variables. In their study on Evaluation of Information Security Management System Success Factors: Case Study of Municipal organization, Kazemi, Khajouei and Nasrabadi (2012), used a cross-sectional survey design. Kock and Ellstrom (2010) used Formal and Integrated Strategies for Competence Development in SMEs also used a cross-sectional survey design.

The study was also guided by an epistemological research philosophy. Research philosophy relates to the development of knowledge and the nature of that knowledge (Saunders, Lewis &

Thornhill, 2009). There are three epistemological positions: realism, interpretivism and positivism (Saunders, Lewis & Thornhill, 2009). This study adopted a positivist research paradigm which is an epistemological position. Positivism is characterized by a belief in theory before research and statistical justification of conclusions from empirically testable hypothesis, the core of tenets of social science (Cooper & Schindler, 2011). Epistemological research in the positivist paradigm is how the social world can be investigated as natural science (Koul, 2008). Hypotheses have to be tested by empirical approaches. Koul posits that since the focus of the positivist paradigm is to discover the ‘truth’ through empirical investigation, the quality standards under this paradigm are validity and reliability.

Bryman (2012), states that the question of what is, or should be regarded as acceptable knowledge in a discipline is the main focus of epistemology, or the study of how knowledge develops. Epistemology is categorized as descriptive where one can describe the philosophical position than can be discerned in research (Bryman & Bell, 2007).

The study by Gordon, Loeb, and Zhou (2011) on “The impact of information security breaches: Has there been a downward shift in costs?” and one by Zafar, Ko and Osei-Bryson (2012) on “Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors” used a positivist research paradigm.

3.3 Population

Zikmund, Babin, Carr, and Griffin (2012) define population as the large collection of all subjects from where a sample is drawn. Kombo and Tromp (2009) define the target population as a group of individuals, objects or items from which samples are taken for measurement. The target population, also known as the unit of observation, for this study were the medium-sized firms in Kenya. The respondents, also known as the unit of analysis, were the IT managers of the 100 medium-sized firms that participated in the 2013 Top 100 Survey. The sampling frame consisted of the medium-sized companies in the services and manufacturing sectors in Kenya that participated in the 2013 Top 100 Survey. Panneerselvam (2006) defined a sampling frame as the complete list of all members or units of the population from which each sampling unit is selected.

3.4 Sample Size and Sampling Technique

Israel (2012) posits that although cost considerations make census technique impossible for large populations, a census is attractive for small populations, for instance, 200 or less. Since the accessible population was the information technology managers of the medium-sized firms in the 2013 top 100 Survey, this study used the entire population as the sample. Israel (2012) further states that a census eliminates sampling error and provides data on all the individuals in the population. The number of respondents were the 100 Information Technology managers, the unit of analysis, assuming one IT manager per medium-sized firm. Therefore, the summary of respondents' sectors was as indicated in Table 3.1.

Table 3.1 Summary of Respondents' sectors (KPMG, 2013)

Stratum	No. of SMEs	Percentage	Proportion Taken
Services	55	55	55
Manufacturing	45	45	45
Total	**100**	**100**	**100**

Kazemi, Khajouei and Nasrabadi (2012) used census in their study on Evaluation of Information Security Management System Success Factors: Case Study of Municipal Organization.

3.5 Data Collection Instruments

Kothari (2009) states that data collection instruments are means by which primary data are collected in social research. There are several ways of collecting data which differ considerably in terms of money costs, time and other resources at the disposal of the researcher (Orodho, 2008). These include questionnaires, mailed questionnaires, observations, personal interviews and telephone interviews. This study used a self-administered, semi-structured questionnaire to obtain primary data. Cooper and Schindler (2011) explain that the questions in a study are directly related to the research questions. Questionnaires consist of a series of specific, short questions that are asked verbally by the interviewer or answered by the respondents on their own (Bryman, 2012). Bryman further explains that the number of closed-ended questions in any survey exceeds the number of open-ended questions.

Lane (2007) used a self-administered, semi-structured questionnaire in the study on Information Security Management in Australian Universities - An Exploratory Analysis.

3.6 Data Collection Procedure

Data collection is the gathering of information to serve or prove some facts (Kombo & Tromp, 2009). The questionnaire was self-administered to the respondents. Secondary data was collected from published sources such as library, internet and research done by other scholars. Chang and Ho (2006) used a self-administered, semi-structured questionnaire in their study on Organizational Factors to the Effectiveness of Implementing Information Security Management. The mail survey has been criticized for nonresponse bias. If persons who respond differ substantially from those who do not, the results do not directly allow one to say how the entire sample would have responded (Armstrong & Overton, 1977).

There are three methods for estimating nonresponse: comparisons with known values for the population, subjective estimates, and extrapolation. This study adopted extrapolation methods which are based on the assumption that subjects who respond less readily (answering later or as requiring more prodding to answer) are more like non-respondents. The most common type of extrapolation is carried over *successive waves* of a questionnaire, where “wave” refers to the response generated by a stimulus, e.g., a follow-up postcard. Berezina, et al., (2012) in their study on the impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth used extrapolation methods for estimating nonresponse bias.

3.7 Pilot Study

Cooper and Schindler (2011) explain that pilot test is conducted to detect weaknesses in design, instrumentation and to provide proxy data for selection of probability sample. The procedures used in pre-testing the questionnaire were identical to those that were used during the actual study or data collection. The number in the pre-test should be small, about 1% to 10% of the target population (Mugenda & Mugenda, 2003). In this study the questionnaire was tested on 10% of the entire sample size, which translated to ten respondents. Boonmak (2008) used pilot study in the study on Influence of Human Factors on Information Security Measures Effectiveness Under Ethic Issues. Sharma and Dash (2012) also, in their study on Effectiveness of ISO 27001 as an Information Security Management System: An Analytical Study of Financial Aspects.

3.7.1 Reliability of Data Collection Instruments

This study adopted the internal consistency method. Reliability is consistency of measurement (Bollen, 1989), or stability of measurement over a variety of conditions in which basically the same results should be obtained. Abbott and McKinney (2013) state that reliability is the extent to which a given measuring instrument produces the same result each time it is used. Typical methods to estimate test reliability in behavioral research are: test-retest reliability, alternative forms, split-halves, inter-rater reliability, and internal consistency (Drost, 2011). The internal consistency method was adopted because it is more stable than the other methods (Bryman, 2012; Cooper & Schindler, 2011). Internal consistency is tested using the Cronbach's alpha statistic. Cronbach's alpha which was popularized by Cronbach (1951), measures consistency within the instrument and assesses how well a set of items measures a particular behavior or characteristic within the test. For a test to be internally consistent, Drost (2011) suggests that estimates of reliability should be based on the average intercorrelations among all the single items within a test. Pallant (2010) advises that where Cronbach's Alpha coefficient is used for reliability test, the value should be above 0.7. Cronbach's alpha (α) was computed as follows:

$$\alpha = K / (K - 1) [1- (\Sigma\sigma_k^2 / \sigma_{total}^2)] \qquad \text{---} \ \text{Equation (1)}$$

where K is the number of items, $\Sigma\sigma_k^2$ is the sum of the k item score variances, and σ_{total}^2 is the variance of scores on the total measurement (Cronbach, 2004). Berezina, Cobanoglu, Miller and Kwansa (2012) used Cronbach's alpha to check the reliability of the data collection instrument in their study on The Impact of Information Security Breach on Hotel Guest Perception of Service Quality, Satisfaction, Revisit Intentions and Word-of-Mouth.

3.7.2 Validity of Data Collection Instruments

This study adopted construct validity. Mugenda and Mugenda (2003) define validity as the degree to which results obtained from the analysis of the data actually represent the phenomenon under study. Validity also refers to the degree to which an instrument measures what it purports to measure (Mugenda, 2008; Bryman, 2012). Validity therefore, is concerned with the meaningfulness of research components. There are four types of validity: statistical conclusion validity, internal validity, construct validity, and external validity (Drost, 2011). Construct validity refers to how well you translated or transformed a concept, idea, or behavior (a construct) into a functioning and operating reality, the operationalization (Trochim, 2006). Abbott and McKinney (2013) concurs and states that construct validity checks whether a measure of a concept relate strongly with another measure that it should strongly correlate with and negatively with measures it should not agree with.

This study also adopted content validity. Content validity is a qualitative type of validity where the domain of the concept is made clear and the analyst judges opine whether the measures fully represent the domain (Bollen, 1989). Drost (2012) posits that there are basically two ways of assessing content validity, that is, ask a number of questions about the instrument or test and/or ask the opinion of expert judges in the field. Exploratory Factor Analysis (EFA) can be used to validate hypothetical constructs by clustering those indicators or characteristics that appear to correlate highly with each other (Kane, 2006). Alfawaz (2011) used construct validity in his study on Information Security Management: A Case Study of an Information Security Culture. Baggili (2009) too in his study on Effects of Anonymity, Pre-Employment Integrity and Antisocial Behavior on Self-Reported Cyber-Crime Engagement: An Exploratory Study.

3.8 Measurement and Scaling Technique

Panneerselvam (2006) defines measurement as the assignment of a number to an object which reflects the degree of possession of a characteristic by that object. This study used open-ended questions and a 5-point Likert scale to measure the objectives. Open-ended questions give a chance to respondents to add information which may not have been included in the closed-ended questions, while the Likert scale, which is essentially an interval scale, is designed to examine how strongly subjects agree or disagree with a statement (Sekaran & Bougie, 2010). The 5-point Likert scale ranged from “Strongly disagree” to “Strongly agree”, and from “Highly significant” to “Quite insignificant”. Likert Scaling is a unidimensional scaling method (Trochim, 2006) whose concepts are generally easier to understand because you have either more or less of it, and that's all. Kothari (2009), on the other hand, explains that 5-point Likert scales are used because they are more reliable and can provide more information. Kimwele, Mwangi and Kimani (2011) in their study on Information Technology (IT) Security Management in Kenyan Small and Medium Enterprises used a 5-point Likert scale. Also Ghotbi and Gharechehdaghi (2012) in their study on Evaluating the Security Actions of Information Security Management System in the Electronic Stock Commerce, and Providing the Improvement Strategies.

3.8.1 Measurement of Independent and Moderating Variables

This study used the following rating scales, that is, a dichotomous scale to elicit a Yes or No answer, open-ended questions to allow the respondents to add information that might not be included in the closed-ended questions and Likert scale, developed by Rensis Likert, to examine how strongly subjects agree or disagree with a statement (Cooper & Schindler, 2011). In this study, Likert scales dominated the questionnaire. Chimi and Russel (2009) elucidated that Likert scale is everywhere in nearly all fields of scholarly and business research that it is used in a wide variety of circumstances: when the value sought is a belief, opinion or effect; when the value sought cannot be asked or answered definitely and with precision; and when the value sought is considered to be of such a sensitive nature that respondents would not answer except categorically in large ranges. The nature of the data that was collected in this study exhibited majority of these features and so the Likert scale was the most suitable. A Likert Scale can be evaluated easily through standard techniques like, factor analysis and logistic regression analysis (Montgomery, Peck & Vining, 2001). All the hypotheses to test the relationship between information security management and firm performance were measured by a linear regression model.

Top management commitment was measured through financial support, participation and end-user satisfaction; Information security policy enforcement was determined by right implementation, acceptance by employees and teamwork; human-related information security issues was determined through culture, training and awareness; and Information Technology competence was determined through knowledge of information systems, experience in information systems and information systems resources. The study used the following formula to determine the risk level:

Risk = (Likelihood of Vulnerability x Value) - % Risk already controlled + element of uncertainty ---Equation (2)

Therefore risk assessment was determined through threats and vulnerabilities, potential impact and likelihood of occurrence. Lastly, the moderating variable used the Likert scale to measure how strongly one agrees or disagrees with the key dimensions that characterize an entrepreneurial orientation: a willingness to innovate and take risks, and a tendency to be proactive relative to marketplace opportunities (Hughes & Morgan, 2007).

3.8.2 Measurement of Dependent Variable

Profitability was used to measure firm performance. Zafar, Ko and Osei-Bryson (2012) used profitability as a measure of firm performance. This was in their study on Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors.

3.9 Data Analysis and Processing

Zikmund et al (2012) posit that data analysis is the application of reasoning to understand the data that have been gathered with the aim of determining consistent patterns and summarizing the relevant details revealed in the investigation. Data processing entails editing, classification and tabulation of data collected so that they are amenable to analysis (Kothari, 2009). Data entry converts information gathered by secondary or primary methods to a medium for viewing and manipulation. IBM Statistical Package for the Social Sciences (SPSS) version 21.0 for Windows 7 and Windows 8 was used for data entry, data cleaning and running the Exploratory Factor Analysis (EFA).

Berezina, Cobanoglu, Miller and Kwansa (2012) used SPSS in their study on the Impact of Information Security Breach on Hotel Guest Perception of Service Quality, Satisfaction, Revisit Intentions and Word-Of-Mouth. Others are Shropshire (2009) in his study on A Canonical Analysis of Intentional Information Security Breaches by Insiders, and Kazemi, Khajouei and Nasrabadi (2012) in their study on Evaluation of Information Security Management System Success Factors: Case Study of Municipal Organization. Other applications software used were Ms-Excel for Windows 8 for case cleaning, variable screening and as a transit package in that the data from SPSS was saved in Ms-Excel first for it to be exported to SmartPLS; Analysis of Moment Structures (AMOS) version 18, which is essentially analysis of mean and co-variance structures, for Initial EFA, Confirmatory Factor Analysis (CFA), generation of fit models, Path Analysis and Structural Equation Modeling (SEM); SmartPLS version 2.0 for Path Analysis, SEM with moderation and model diagnostics; STATA version 12.0 to test for assumptions of the variables used in the analyses; and R-GUI version 2.10.0 for building plots, for instance box-plots using the Ggplot2 package, and for univariate and multivariate testing of outliers in the dependent variable. Lastly, ATLAS was used for qualitative analysis.

Koong, Merhi and Sun (2013), in their study on Push and Pull Effects of Homeland Information Security Incentives, used the SEM software package AMOS for model analyses. Hafiz and Shaari (2013) in their study on Confirmatory Factor Analysis (CFA) of First Order Factor Measurement Model-ICT Empowerment in Nigeria, also used AMOS to test for the measurement models. Bahl and Wali (2014) used SmartPLS to analyze field survey data in their study on Perceived Significance of Information Security Governance to Predict the Information Security Service Quality in Software Service Industry: An Empirical Analysis. Kim, Kim & French (2014) employed structural equation modeling (SEM) using SmartPLS 2.0 to analyze the measurement model in their study on What Increases Firms' Performance of Information Security Management and the Role of Regulatory Pressure. Latip, Salleh, Omar and Yaakub (2013) analyzed the data for CFA using SmartPLS 2.0 software.

This study employed descriptive statistics to analyze qualitative data. The purpose of descriptive statistics is to enable the researcher to meaningfully describe a distribution of scores or measurements using a few indices or statistics (Mugenda & Mugenda, 2003), with the types of statistics or indices used being dependent on the type of variables in the study and the scale of measurement used: nominal, ordinal, interval or ratio.

Most statistical tests rely upon certain assumptions about the variables used in the analysis. When these assumptions are not met the results may not be valid, resulting in either Type I or Type II error, or over- or under-estimation of significance or effect size(s) (Osborne & Waters, 2002). Pedhazur (1997) noted that knowledge and understanding of the situations when violations of assumptions lead to serious biases and when they are of little consequence are essential to meaningful data analysis. However, as Osborne, Christensen, and Gunter (2001) observe, few articles report having tested assumptions of the statistical tests they rely on for drawing their conclusions, putting validity of their results into question. This study satisfactorily tested assumptions of the statistical tests.

This study tested for normality, heteroscedasticity and autocorrelation. Normality is important in knowing the shape of the distribution and helps to predict dependent variables scores (Paul & Zhang, 2009). Heteroscedasticity means a situation in which the variance of the dependent variable varies across the data, as opposed to a situation where Ordinary Least Squares, OLS, makes the assumption that $V(\varepsilon_j)=\sigma^2$for all j, meaning that the variance of the error term is constant (homoscedasticity). Heteroscedasticity complicates analysis because many methods in regression analysis are based on an assumption of equal variance (Park, 2008). Autocorrelation refers to the correlation of a time series with its own past and future values (Box & Jenkins, 1976). The autocorrelation function can be used to detect non-randomness in data and also to identify an appropriate time series model if the data are not random. Autocorrelation is essentially a correlation coefficient, but instead of correlation being between two different variables, the correlation is between two values of the same variable at times X_i and X_{i+k}.

To test for normality, heteroscedasticity, and serial correlation (autocorrelation) of regression residuals, this study used STATA version 12.0 software. Koong, Merhi and Sun (2013) used STATA software to test for assumptions on variables used in their analyses in their study on Push and Pull Effects of Homeland Information Security Incentives.

This study also tested for multicollinearity. Multicollinearity is the undesirable situation where the correlations among the independent variables are strong (Martz, 2013). To test for multicollinearity, Variance Inflation Factor (VIF) was used. If no two independent variables are correlated, then all the VIFs will be 1. If VIF for one of the variables is around or greater than 5, there is multicollinearity associated with that variable. In this case one of these variables must be removed from the regression model (Cohen, Cohen, West & Aiken, 2003). Knapp (2005) tested for multicollinearity in his study on A Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test. Cavusoglu, Mishra and Raghunathan (2004) also tested for multicollinearity in their study on The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers.

Structural equation modeling (SEM) was used for model analyses (Schumacker & Lomax, 1996), including testing for the hypothesized relationships in this study. These were the null hypotheses that top management commitment, information security policy enforcement, human-related information security issues (culture, awareness and training), information technology competence, and information security risk assessment have no relationship with firm performance in Kenya and the null hypothesis that entrepreneurial orientation does not moderate the influence of information security management on firm performance in Kenya. The study used t-statistics to test whether the hypothesized model was significant at 80% significance level.

This study also used the Exploratory Data Analysis (EDA). EDA is an approach/philosophy for data analysis that employs a variety of techniques (mostly graphical) to maximize insight into a data set; uncover underlying structure; extract important variables; detect outliers and anomalies; test underlying assumptions; develop parsimonious models; and determine optimal factor settings (Bordens & Abbort, 2014). In this study, EDA was used to reveal the data structure, assess whether the assumptions are met before any further statistical inferences are done, and detect outliers.

Abbott and McKinney (2013) define an outlier as an extreme case that distorts the true relationship between variables, either by creating a correlation that should not exist or suppressing a correlation that should exist. Miles and Shevlin (2001) posit that outliers are aberrant scores that lie outside the usual range of scores we would expect for a particular variable. In multivariate data, outliers for ordinal variables are those units representing an unusual combination of the categories or of the ranks of the variables (Riani, Torti & Zani, 2012).

The outliers were tested in this study through computing Mahalanobis distance for each sample, with outliers being identified as those samples yielding large values of Mahalanobis distance (Webb & Copsey, 2011). The Mahalanobis distance is calculated from the leverage value; the advantage of the Mahalanobis distance is that it is possible to use the distances as a value with a known distribution, which can then be tested for significance, by finding its associated probability (Miles & Shevlin, 2001). For cases with multiple independent variables, it is calculated using:

$\mathrm{MD}_\mathrm{i} = (N - 1)\ (h_i - (1/N))$, --Equation (3)

where h_i is the leverage statistic for the *i*th case and N is the number of participants. R-GUI version 2.10.0 software was also used for building box plots and for univariate and multivariate testing of outliers in the dependent variable. In his study on A Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test, Knapp (2005) tested for outliers.

Exploratory Factor Analysis (EFA) was employed in order to identify the constructs that were then be regressed against the dependent variable (Cooper & Schindler, 2003). Berezina et al (2012) used EFA in their study on The Impact of Information Security Breach on Hotel Guest Perception of Service Quality, Satisfaction, Revisit Intentions and Word-Of-Mouth. Chang and Ho (2006) too in their study on Organizational Factors to the Effectiveness of Implementing Information Security Management. Prior to the EFA were the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and the Bartlett's test of sphericity. These tests were conducted to confirm whether there was a significant correlation among the variables to warrant the application of EFA (Snedecor & Cochran, 1989).

The KMO statistics vary between 0 and 1 (Argyrous, 2005). A value of zero indicates that the sum of partial correlation is large relative to the sum of correlations indicating diffusions in the patterns of correlations, and hence that factor analysis likely to be inappropriate (Costello & Osborne, 2005). A value close to 1 indicates that the patterns of correlations are relatively compact and so factor analysis should yield distinct and reliable factors (Cooper & Schindler, 2011). Bartlett's Test of Sphericity tests the hypothesis that one's correlation matrix is an identity matrix, which would indicate that the variables are unrelated and therefore unsuitable for structure detection. Small values ($p < 0.05$) of the significance level indicate that a factor analysis may be useful with one's data. The values obtained from the two tests indicated factor analysis to be appropriate. Chang and Ho (2006) used the KMO in their study on Organizational Factors to the Effectiveness of Implementing Information Security Management.

Additionally, Principal Component Analysis (PCA) was employed to decompose the variations in the multivariate data set into a set of components such that the first component accounts for as much of the variations in the data as possible (Abdi & Williams, 2010). In his study on A Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test Knapp (2005) tested for PCA. Eigen values were used to determine the factor loadings for each component. The larger the eigen value, the more important the associated principal component (Graham & Midgley, 2000).

In order to test the relationship between information security management and firm performance, the model fitness, significance of results and consequently the validity of findings, Structural Equation Modeling (SEM) analysis was done (Cooper and Schindler, 2003). It is a common mistake to think of SEM as an esoteric method that is difficult to learn and use. In reality, the substance of SEM to a larger extent lies with the ease with which it allows non-specialists to solve estimation and hypothesis testing problems that were once thought of as a preserve of statisticians (Bhattacharyya, 2011). Put another way, SEM is a multivariate analysis technique that subsumes standard methods, including regression, factor analysis, simultaneous equations, and analysis of variance. Bhattacharyya further adds that many researchers are now going beyond traditional techniques such as EFA and regression to explore complex relationship.

When data is analyzed using an SEM approach, a hypothesis is formulated about the underlying model and that hypothesis is tested (Miles & Shevlin, 2001). Additionally, the most powerful aspect of SEM is the ability to correct for measurement error. SEM is also quite flexible. Analysis of Moment Structures (AMOS) software makes SEM easy. Indeed apart from using SEM to confirm and explain conception model that involve attitudes and perceptions, AMOS also implements analysis of covariance structures, or causal modeling (Argyrous, 2005). This study used AMOS to construct a conceptual model linking the variables under study.

Accordingly, the study employed Confirmatory Factor Analysis (CFA) and SEM, in particular the path analysis, to construct the linkage between the dimension of information security management and firm performance (Pearl, 2000). In their study on Impacts of Organizational Capabilities in Information Security, Hall, Sarkani and Mazzuchi (2011) used confirmatory factor analysis to evaluate measurement model on multiple criteria, structural equation modeling to fit a theoretical model, and AMOS as a tool for analyzing data and conducting SEM.

Lastly, in order to test the effects of the moderating role of entrepreneurial orientation, the study employed hierarchical regression analysis with moderation. In hierarchical multiple regression analysis, the researcher determines the order that variables are entered into the regression equation (Tabachnick & Fidell, 1989). Montiel-Campos, Solé-Parellada, Aguilar-Valenzuela, Berbegal-Mirabent and Duran-Encalada (2011) in their study on The Impact of Moral Awareness on the Entrepreneurial Orientation-Performance Relationship in New Technology-Based Firms used hierarchical regression analysis.

3.9.1 Common Method Variance

Common-method variance (CMV) is a systematic error variance shared among variables measured with and introduced as a function of the same method and/or source (Richardson, Simmering and Sturman, 2009). It is the spurious variance that is attributable to the measurement method rather than to the constructs the measures represent (Podsakoff, MacKenzie, Lee and

Podsakoff, 2003). Method biases are a problem because they are one of the main sources of measurement error. Measurement error threatens the validity of the conclusions about the relationships between measures and is widely recognized to have both a random and a systematic component, Nunnally (1978) as cited in (Podsakoff et al., 2003). Although both types of measurement error are problematic, systematic measurement error is a particularly serious problem because it provides an alternative explanation for the observed relationships between measures of different constructs that is independent of the one hypothesized.

One of the main sources of systematic measurement error is method variance that may arise from a variety of sources such as content of specific items, scale type, response format, and the general context. However, regardless of its source, systematic error variance can have a serious confounding influence on empirical results, yielding potentially misleading conclusions (Richardson et al, 2009). To test for common method variance, three ex post techniques can be used: the correlational marker technique, the confirmatory factor analysis (CFA) marker technique, and the unmeasured latent method construct (ULMC) technique (Richardson et al, 2009).

This study used the CFA marker technique because of its ability to model random error in the marker and substantive constructs and the ability to model common method variance at the item level, and thus the ability to account for noncongeneric and congeneric common method variance (Williams, Hartman, & Cavazotte, 2003). Berezina, Cobanoglu, Miller & Kwansa (2012) in their study on The Impact of Information Security Breach on Hotel Guest Perception of Service Quality, Satisfaction, Revisit Intentions and Word-of-Mouth, used CFA marker approach to test for common method variance.

3.10 Statistical Model and Hypothesis Testing

Moderated multiple regression (MMR) statistical tool was used to test whether entrepreneurial orientation moderates the relationship between information security management and firm performance (Aguinis & Gottfredson, 2010). Moderated multiple regression is suited to this study because it enables the slope of one or more of the independent variables to vary across values of the moderator variable, thereby facilitating the investigation of an extensive range of relationships and function forms (Goode & Harris, 2007). Moderated multiple regression also permits the multiple relationships between the endogenous variable and exogenous variables to depend on the levels of the other exogenous variables in the study.

Estimating interaction effects using moderated multiple regression usually consists of creating an ordinary least squares (OLS) model and a moderated multiple regression (MMR) model equations involving scores for a continuous predictor variable Y, scores for a predictor variable X, and scores for a second predictor variable Z hypothesized to be a moderator (Aguinis & Gottfredson, 2010). To determine the presence of moderating effect, the OLS model was then compared with the MMR model. Shropshire (2009) used moderated multiple regression in his study on A Canonical Analysis of Intentional Information Security Breaches by Insiders.

The first equation which showed the ordinary least squares (OLS) regression equation for a model predicting y scores from the first-order effects of X and Z observed scores was:

$y = \beta_0 + \beta_1 X + \beta_2 Z + \varepsilon$ --Equation (4)

where β_0 = least squares estimate of the intercept, β_1 = least squares estimate of the population regression coefficient for X observed scores, β_2 = least squares estimate of the population regression coefficient for Z observed scores, and ε = error term.

The second equation, the moderated multiple regression model was formed by creating a new set of scores for the two predictors (i.e. X, Z), and including it as a third term in the equation, which yielded the following model:

$y = \beta_0 + \beta_1 X + \beta_2 Z + \beta_3 X{*}Z + \varepsilon$ ---Equation (5)

where β_3 is the least squares estimate of the population regression coefficient for the interaction term scores. T-statistic was used to test the significance of the variable weights. Appropriate alphas were used for assessment at the different significance levels.

CHAPTER FOUR

RESEARCH FINDINGS AND DISCUSSION

4.1 Introduction

The main objective of this chapter was to provide the analyses of the results, interpretation of the results and findings. In this chapter, qualitative analysis of the open-ended questions was undertaken. Also, several steps were embarked on towards ensuring building of a good quantitative model, as well as key general guidelines for structuring a quantitative model. In general, analyses were conducted using a two-phase process consisting of confirmatory measurement model and confirmatory structural model.

4.2 Response Rate

The targeted respondents in the study were Information Technology Managers of the medium-sized companies that participated in the 2013 Top 100 Survey. A total of 94 questionnaires were returned. 6 SMEs declined to participate in the survey, out of which 3 claimed they had "no-survey" policy, while the rest just could not participate at the time. This resulted in a response rate of 94%. Babbie (1990) stated that a response rate of 50% is adequate while Bailey (1987) set an adequate response rate at 75%. Mugenda (2008) avers that a response rate of 50% is adequate, 60% and above good, and above 70% very good. Therefore a response rate of 94%, cognizant of the sensitive nature of the study, is quite adequate. The response was higher in the services sector than in the manufacturing sector. This was because of the limited physical access allowable in manufacturing firms as compared to their services counterparts. Majority of related studies realize very low response rates.

In a related study on Impacts of Organizational Capabilities in Information Security by Hall, Sarkani and Mazzuchi (2011), a response rate of 27% was realized. In another study by Kim (2014) on Recommendations for Information Security Awareness Training for College Students, a response rate of 19.6% was realized. In yet another related study on Information Security in the South Australian Real Estate Industry by Mani, Choo and Mubarak (2014) the response rate was 29%. Only very few studies cross the 50% mark. For instance, the study by Upfold and Sewry (2005) on An investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape realized a response rate of 86.5%, though this could be attributed to the small size of the sample at 37, out of which 32 responded. Table 4.1 summarizes the response rate in this study.

The low response rate recorded by the scholars in the above three studies could be attributed to mailing the data collection instruments to the respondents in lieu of self-administering them. Some people do not read their electronic mails regularly while others could have changed their e-mail addresses, and yet others could be lazy in responding to mails. If mailed by post, inefficiency of the service could result into low response rate. Self-administering on the other hand means meeting face-to-face with your respondents who, more often than not, would respect the effort made in reaching them. Self-administering was used in this study.

Table 4.1 Response Rate

SME Sector	Questionnaires Distributed	Questionnaires Received	% Response
Services	55	53	96.4
Manufacturing	45	41	91.1
Total	**100**	**94**	**94**

4.3 Firm Demographics

The demographic characteristics of the medium-sized companies in the 2013 Top 100 Survey was collated and reviewed. The analysis was based on the information that the respondents provided in the questionnaire. The firm's subsector, number of years worked, number of people employed, average turnover and number of computers in use in the firm were captured, and the results shown in table 4.2.

The subsectors were in only two categories of services and manufacturing with services firms being more in number in the survey than the manufacturing firms. Majority (68%) of the respondents had worked for a period ranging from one to five years. This shows a high turnover of employees in the information technology department, meaning that people with IT skills or competence are highly sought after by employers, and that employers nowadays are taking information security issues seriously. Majority (54.3%) of the firms employed less than fifty employees, while 39.8% of the firms recorded an average turnover of between KES. 101-200 million. Equally, 39.8% of the firms recorded an average turnover of between KES. 201-1,000 million per annum. On average, the number of computers in a firm, irrespective of the sector, was 24. The results of the demographic survey show a high turnover of employees in the information technology department, meaning that people with IT skills or competence are highly sought after by employers. This is a demonstration that employers nowadays are taking information security issues seriously.

Table 4.2 Firm Demographics

Main Factor	Factor Level	Mean (se (µ))	Frequency	Percent
Sub-sector	Services	-	53	56.4
	Manufacturing		41	43.6
	Other		0	0.0
Length of Time (Years) Worked as an IT Manager	0-Less than 1	-	0	0.0
	1-5		64	68.1
	6-10		26	27.7
	More than 10		4	4.3
Number of People Employed	0-9	-	0	0.0
	10-49		51	54.3
	50-250		43	45.7
Average Turnover (in millions)	0-50	-	1	1.1
	51-100		18	19.4
	101-200		37	39.8
	201-1000		37	39.8
Number of Computers Used		24 (±2)		

4.4 Correlations of the Study Variables

Correlation among the independent variables is illustrated by the correlations matrix in table 4.3. Correlation is often used to explore the relationship among a group of variables (Pallant, 2010), in turn helping in testing for multicollinearity. That the correlation values are not close to 1 or -1 is an indication that the factors are sufficiently different measures of separate variables (Farndale, Hope-Hailey & Kelliher, 2010). It is also an indication that the variables are not multicollinear. Absence of multicollinearity allows the study to utilize all the independent variables.

Table 4.3 shows that the lowest correlation in this study was between information security policy enforcement and top management commitment (r=0.466, p<0.01). The highest correlation was between human-related information security issues and information security policy enforcement (r=0.875, p<0.01). A correlation of above 0.90 is a strong indication that the variables may be measuring the same thing (Tabachnick & Fidell, 2013). The fact that all the correlations were less than 0.90 was an indication that the factors were sufficiently different measures of separate variables, and consequently, this study utilized all the variables.

Table 4.3 Correlations of the Study Variables

Variables	TMC	ISPE	HRI	ITC	ISRA	EO
TMC	1	.466**	.456**	.566**	.470**	.466**
ISPE	.466**	1	.875**	.695**	.735**	.550**
HRI	.456**	.875**	1	.699**	.771**	.568**
ITC	.566**	.695**	.699**	1	.699**	.642**
ISRA	.470**	.735**	.771**	.699**	1	.529**
EO	.466**	.550**	.568**	.642**	.529**	1

N ranges from 88 - 94 ** Correlation is significant at the 0.01 level (2-tailed).

4.5 Description of Factors of the Study Variables

The description of the factors of the study variables is shown Appendix V. This description was quite helpful in cross referencing since the factors were used in data analyses, model analyses, and throughout the entire study. With the exception of human-related information security issues and firm performance variables which had 5 factors each, the rest of the variables, that is, top management commitment, information security policy enforcement, IT competence, information security risk assessment, and entrepreneurial orientation had 7 factors each. In total there were 45 factors.

4.6 Descriptive and Qualitative Analysis of the Study Variables

The research instrument was divided into 3 sub-sections for each of the research variable. The first two sub-sections consisted of closed and open ended questions. These questions provided respondents with two alternatives of either responding in the affirmative or in the negative. The affirmative answer required the respondent to tick the "Yes" box while the negative response required an explanation. The explanations were further subjected to qualitative analysis. Qualitative analysis involved several stages, *inter alia*, sorting and classification, open coding, axial coding, and select coding. This resulted in a fewer questions being analyzed as some could not meet the threshold. In the third sub-section, all respondents were subjected to a Likert table. In this way, every aspect of the variable was addressed and consequently analyzed. Bakari (2007) used the same format in his study on A Holistic Approach for Managing ICT Security in Non-Commercial Organizations - A Case Study in a Developing Country. Alfawaz (2011) also used the same format in his study on Information Security Management: A Case Study of an Information Security Culture.

4.6.1 Analysis of Top Management Commitment Amongst Top 100 Medium-sized Firms

Top management commitment was operationalized into financial support, management participation and user satisfaction.

Majority (69.1%) of the firms considered information security budgetary allocation as one of the vital components of the overall budget, while a few (30.9%) did not, as shown in table 4.4. Although it is a known fact that majority of the small and medium enterprises face tight constraints on money and resources (Makumbi, Miriti & Kahonge, 2010) the fact that a third of the firms did not consider information security budgetary allocation as one the vital components of the overall budget was worrying. Ignoring information security budgetary allocation in the overall budget could also be one of the reasons why almost 50% of the top 100 medium-sized firms do not appear in the in the subsequent list of Top 100 Survey.

Table 4.4 Consideration of Information Security Budgetary Allocation in the Medium-sized Firms

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	29	30.9	30.9	30.9
	Yes	71	69.1	69.1	100.0
	Total	94	100.0	100.0	

When asked why they did not consider information security budgetary allocation as one of the vital components of the overall budget, this study established that majority (33.33%) of the respondents did not consider information security as a core activity in their firm, another 33.33% said they operated on limited resources, and yet another 33.33% said their firms did not have a well-established IT department. These results are shown in figure 4.1 which indicates the reasons why security budgetary allocation is not considered vital component of the overall budget. The results corroborate a study by Okpara (2011) on Factors Constraining the Growth and Survival of SMEs in Nigeria: Implications for Poverty Alleviation, in which he found that many of the small businesses are dogged by management problems, including accounting, finance, personnel, and management issues, and which eventually could cause business failure. However, the extent to which limited financial resources solely are a major obstacle to business development is still contentious. For instance, Dia (1996) in her book titled African Management in the 1990s and Beyond: Reconciling Indigenous and Transplant Institutions, observed that additional capital was not necessarily required to carry out a successful business activity and that lack of capital could be compensated through innovation. This means that many of the problems faced by small businesses could be solved through the ability to generate ideas that will culminate in the production of new products, services and technologies, including technological entrepreneurship.

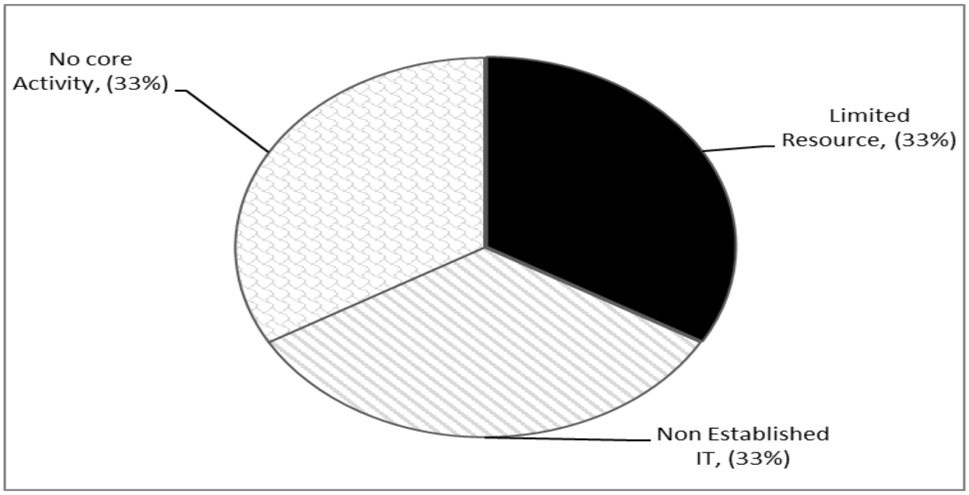


Figure 4.1 Reasons Why Security Budgetary Allocation is not Considered Vital Component of the Overall Budget

On being asked whether information security was discussed regularly as one of the important agendas in their senior total quality management meetings, majority (85%) of the respondents answered in the affirmative while a few (15%) responded in the negative, as shown in table 4.5. The number of respondents who answered in the affirmative is relatively high at 85%, showing that majority of the top 100 medium-sized firms surveyed have realized the importance of keeping abreast with the security situation. This is a demonstration of entrepreneurial leadership, whereby the leaders in these medium-sized firms forge an organizational unit that is constantly repositioning it to capture opportunistic rents. Also, discussing information security in the senior total quality management meetings is indicative of an entrepreneurial mindset of the leaders as well as managers and employees who are determined to position their firms at the top of the game in a competitive landscape.

Saint-Gemain (2005) in his study on Information Security Management Best Practice Based on ISO/IEC 17799 found out that effective information security requires the active involvement of executives and should not be regarded as a technical issue to be relegated to the information technology (IT) department. Information security should be treated as a business and governance challenge that must be addressed at the highest levels of the organization (ITGI, 2006). This might change the business model of a firm prompting it to collaborate with external partners in order to innovate successfully, develop new sources of income, and probably reach more profitable positions in the competitive landscape.

Table 4.5 Discussion of Information Security in Senior Management Meetings

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	14	14.9	14.9	14.9
	Yes	80	85.1	85.1	100.0
	Total	94	100.0	100.0	

When the respondents were asked why information security was not discussed regularly as one of the important agendas in their senior TQM meetings, it was established that majority (50%) of the respondents did not consider information security as a priority in their firms, 36% claimed to have limited resources, a few (7%) said they do not have an established IT department and yet another 7% claimed lack of knowledge. The results are shown in figure 4.2 which indicates the reasons why information security was not discussed regularly in management meetings.

This was a further demonstration of the range of factors and obstacles faced by small and medium enterprises, which could be solved through innovation (Dia, 1996). Certainly what the small entrepreneurial firm lacks in resources should be made up for in its specialized expertise, personalized attention and innovation in the sense of inventing to deal with the resource constraints that the firm faces (Manalova, Brush, Edelman, & Greene, 2002). Thus, and departing from some of the reasons given above, the essence of entrepreneurship is the capability of a firm’s management to profit from the uncertainty, and creating and pursuing opportunities without concern to the resources under the firm’s control at that moment in time (Stevenson & Jarillo, 1990).

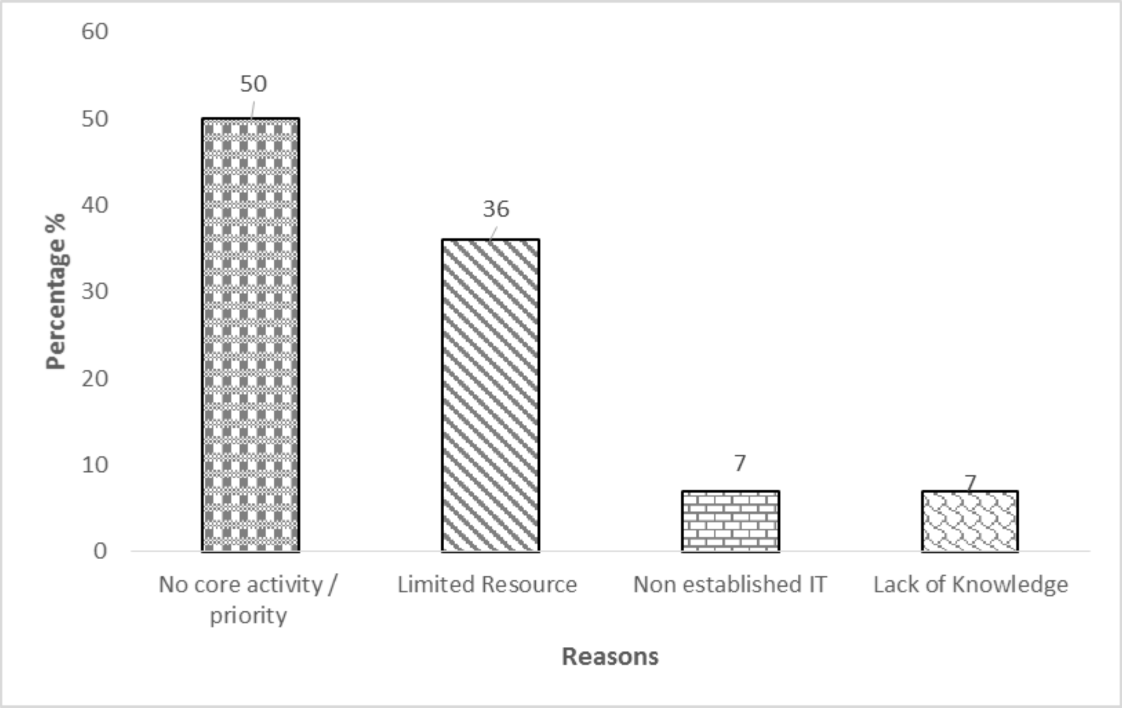


Figure 4.2 Reasons Why Information Security was not Discussed Regularly in Management Meetings

Respondents were also required to address the question of whether employees complained about security rules. Majority (66%) of the respondents said their employees did not complain about security rules, while a few (34%) said they did, as shown in table 4.6. The access to Internet is too tempting and too interesting for employees that quite a number of them would prefer unrestricted access. Free access to all the more interesting social media sites does not make the situation any better. Nevertheless, with 66% of the employees not complaining is indicative of the high level of discipline maintained by employees of the top 100 medium-sized firms.

Table 4.6 Complaints of Employees about Security Rules

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	62	66.0	66.0	66.0
	Yes	32	34.0	34.0	100.0
	Total	94	100.0	100.0	

When asked why employees complained about security rules, majority (50%) of the respondents claimed they restricted access, especially of the Internet because unrestricted access affected performance, 37% said they only limited access to Internet and some sites, but still employees complained, while a few (13%) claimed they restricted access to avoid virus infections and to improve security. Since SMEs face several constraints in conducting business, with a major liability being lack of financial resources and technical capabilities (Vanhaverbeke, Vermeersch & de Zutter, 2012), the last thing that managers would expect to find is an employee who is not serious with work. Internet could be used in many useful ways, including seeking collaborations with other firms for open innovation, leading to higher profitability levels. It is therefore in the interest of the firm, as far as the managers are concerned, to limit time of access and access to some risky sites. The results are in figure 4.3 which indicates the reasons for complaints about security rules.

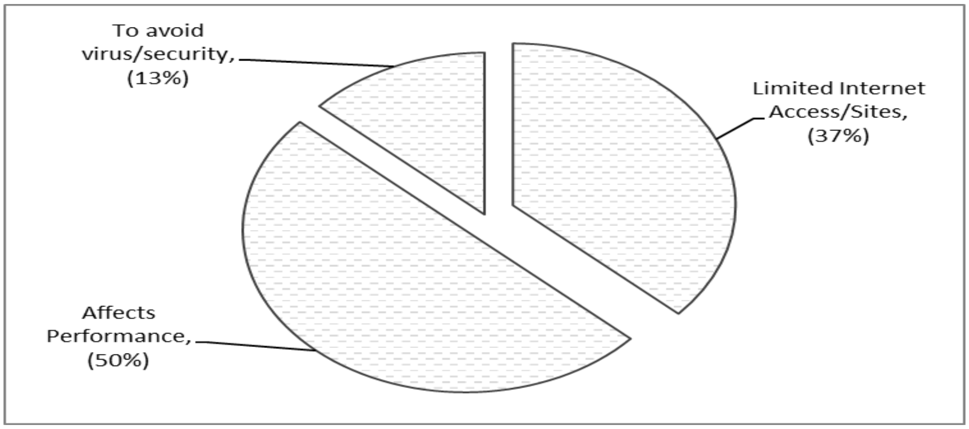


Figure 4.3 Reasons for Complaints about Security Rules

Measurement of Financial Support Factor Amongst Medium-sized Firms

Financial support was measured using the Likert scale and the results, expressed as percentages, as shown in table 4.7. The results showed that majority (77.7%) of the respondents agreed that top management gives satisfactory budget allocation to the security program, 13.8% were neutral while a few (8.5%) disagreed. Still on financial support, the study sought to find out whether top management allocated supplementary/additional budget to the security program when need arises. In this instance, majority (86.2%) agreed, 8.5% were neutral while a few (5.3%) disagreed.

Managing resources strategically is a dimension of strategic entrepreneurship. Resources could be the basis of top 100 medium-sized firms' differential performances in terms of wealth creation. Research has shown that a firm's use of particular resources, particularly financial capital, has a stronger influence on performance than do industry characteristics (Barney &

Arikan, 2001). These results are supported by resource-based view theory which states that firm performance is determined by the resources it owns, and that the firm with more valuable scarce resources is more likely to generate sustainable competitive advantages (Liang, You & Liu, 2010).

On the flipside, a study by Dojkovski, Lichtenstein and Warren (2007) on Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia, found out that while SMEs generally lack funds to coordinate and manage security activities, SME owners themselves are not supportive of information security in terms of time and budget, a clear indication of low budgetary support for IT security within some of the organizations. This could lead to low levels of research, leading to even lower levels of innovation, eventually culminating into low firm performance.

Table 4.7 Response on Financial Support Factors

Financial Support Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
TMC1	%	6.4	2.1	13.8	71.3	6.4	3.69	0.880
TMC2	%	2.1	3.2	8.5	79.8	6.4	3.85	0.671

Measurement of Management Participation Factor Amongst Medium-sized Firms

Using the Likert scale, the results of the measurement of management participation factor are shown in table 4.8. Emanating from the results, majority (80.9%) of the respondents were of the opinion that top management participation is a signal to other employees of how to value information security initiatives, a few (4.3%) disagreed, while 14.9% were neutral. This is indicative of entrepreneurial leadership as it is characterized by an imperative of supporting an entrepreneurial capability (Covin & Slevin, 2002). On whether the results of information security evaluation were reviewed with staff and reported to the Board of Directors, majority (72.4%) agreed to the opinion, a few (12.8%) disagreed while 14.9% were neutral. The percentage of the respondents who disagreed and remained neutral is unsettling, standing at almost a third of the respondents.

As noted by Abu-Musa (2010) in his study on Information Security Governance in Saudi Organizations: An Empirical Study, boards of directors should increasingly be expected to make information security an inherent part of the enterprise's governance efforts, much as the executive management has the responsibility to consider and respond to information security issues. Undoubtedly, organizations should consider the impact on reputation and enterprise value resulting from information security failures (ITGI, 2006).

Majority (85.1%) of the respondents agreed to the opinion that top management is always willing to learn and to be informed on vital information security issues. But a few (7.5%) disagreed while 7.4% were neutral. Nevertheless, it is still worrying that in many cases, small business owners are simply unclear as to what steps they should take or even where to start as far as safeguarding their businesses are concerned (Makumbi, Miriti & Kahonge, 2012). Medium-sized companies in Kenya face substantive competition from multinational firms and amongst themselves. This calls for entrepreneurial leadership in order to withstand operations in a business environment that is highly unpredictable and in which competitive action rapidly erodes whatever advantage a medium-sized firm may be holding dear.

Table 4.8 Response on Management Participation Factors

Management **Participation Factors**		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
TMC3	%	1.1	3.2	14.9	68.1	12.8	3.88	0.701
TMC4	%	4.3	8.5	14.9	68.1	4.3	3.60	0.872
TMC5	%	4.3	3.2	7.4	76.6	8.5	3.82	0.803

Measurement of User Satisfaction Factor Amongst Medium-sized Firms

The results of user satisfaction are shown in table 4.9. When asked whether user satisfaction represents the success of various managerial interventions designed to promote end-user adoption, majority (89.3%) agreed with this opinion, a few (3.2%) disagreed while 7.4% were neutral. This is in line with the study by Liang, et al (2007) who, in their study on Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management, who attributed user satisfaction to the success of various managerial interventions. User satisfaction comes mostly with the availability of appropriate resources. This availability could only be possible with the approval of adequate budget by the management. This satisfaction would make employees more creative and innovative in their undertakings, leading to increased entrepreneurial intensity levels in the top 100 medium-sized firms.

Respondents were also required to address the question of whether employees value the importance of security. Majority (89.3%) agreed that employees value the importance of security, a few (4.2%) disagreed while 6.4% were neutral. But as Sharma and Yetton (2003) found out, if top management do not show obligation towards information security, that is, entrepreneurial leadership, those below them would follow suit. Therefore it should be the responsibility of top management to lead from the front and encourage those below them.

Table 4.9 Response on User Satisfaction Factors

User Satisfaction Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
TMC6	%	1.1	2.1	7.4	78.7	10.6	3.96	0.603
TMC7	%	2.1	2.1	6.4	75.5	13.8	3.97	0.695

4.6.2 Analysis of Information Security Policy Enforcement

Information security policy enforcement was operationalized into right implementation, acceptance by employees and teamwork. Asked whether information security policies are written in a manner that is clear and understandable, majority (90.4%) of the respondents said yes while a few (9.6%) said no as shown in table 4.10. As Barman (2002) pointed out, the first step in securing an entity's electronic data and system is to design and implement a security policy, as policies define what is being protected and what type of restrictions should be put in place. A study by Kimwele, Mwangi and Kimani (2010) found out that only 47.6% of respondents agreed that they have a well-documented IT security policy and that 42.9% accepted that they lacked documented security policies. In contrast, the current study had a smaller number of respondents lacking documented security policies. This could be attributed to dealing with the topmost medium-sized firms in the country. The study by Makumbi, Miriti and Kahonge (2012) on the other hand found out that there were attempts to develop security policies within SMEs but the implementation was the problem as it was poorly done. This hinders firms from pursuing open innovation, in turn making the firms less competitive especially if they have intentions of internationalizing.

Table 4.10 Consideration of Clarity of Information Security Policies

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	9	9.6	9.6	9.6
	Yes	85	90.4	90.4	100.0
	Total	94	100.0	100.0	

Respondents gave various reasons why information security policies were not written in a manner that is clear and understandable. Majority (70%) of them claimed information security policy documents do not exist in their firms in the first place, 20% claimed it is due to poor planning while a few (10%) said they lack necessary skills, as shown in figure 4.4. As Al-Awadi (2009) pointed out, performance of an organization would improve with the existence of a policy which is acceptable to the employees and followed by the same employees. On the other hand, operational security policy needs have to compete with the initiatives for efficiency and quality customer service. In the absence of this, the employer is likely to blame employees for low entrepreneurial intensity levels in the organization while the problem lies elsewhere: absence of information security policy document.

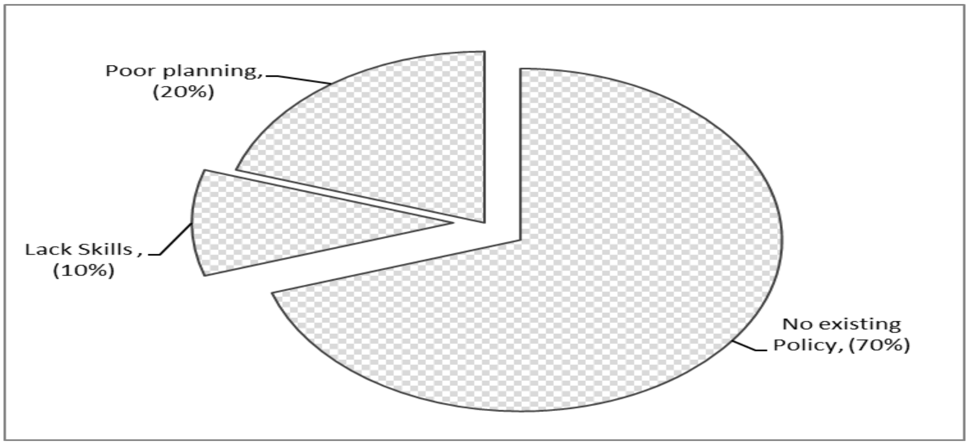


Figure 4.4 Reasons for not having Information Security Policies Written in a Clear and Understandable Manner.

Majority (95.7%) of the respondents were in agreement that necessary efforts were being made to educate new employees about current security policies as shown in table 4.11. A study by Renaud and Goucher (2012) on Health Service Employees and Information Security Policies: An

Uneasy Partnership?, found that even after training, there were instances where it was found that staff were unable to function in a secure manner as they had not understood the training they had undergone. This calls for research before training is conducted in order to determine the level and appropriateness of training. Done innovatively, this should be a sure way of reducing security incidents drastically, thus translating into better firm performance. Only a few (4.3%) of the respondents were not in agreement that necessary efforts were being made to educate new employees about current security policies. This could be attributed to those companies that were not experiencing employment growth. In the study by Kimwele et al (2010), only 28.6% of the respondents agreed that their staff received training in IT security, also an indicator of low employment levels.

Table 4.11 Educating New Employees about Current Security Policies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	4	4.3	4.3	4.3
	Yes	90	95.7	95.7	100.0
	Total	94	100.0	100.0	

Respondents were also required to indicate whether employees in their firms had been trained to regard information security policies as the main tool for achievement of information security management activities. Majority (87.2%) of the respondents answered in the affirmative, a few (10.6%) responded in the negative while 2.1% did not respond, as show in table 4.12. Smith

(2004) avers that in order to identify security threats and proprietary information employees need to be properly trained. Smith further posits that with obligatory training, employees will learn how to interpret the security policy guidelines properly and be able to know what to do in case of a security attack. A study by Njoroge and Gathungu (2013) on The Effect of Entrepreneurial Education and Training on Development of Small and Medium Size Enterprises in Githunguri District – Kenya, found that entrepreneurial education and training reinforces knowledge, skills and attitudes, in turn inculcating managerial skills for running successful enterprises. In short, entrepreneurial training of employees results in superior firm performance. Such training will also enable employees of medium sized firms to participate in policy formulation and implementation. Additionally, an information security policy protects organizational assets and reduces threats (Doherty & Fulford, 2005). Therefore it will help to reduce threats, and it is only reasonable for top 100 medium-sized firms to have a documented policy to reduce their reported level of breaches, and in turn increase performance levels.

Table 4.12 Training on Information Security Policies

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	10	10.6	10.9	10.9
	Yes	82	87.2	89.1	100.0
	Total	92	97.9	100.0	
Missing	System	2	2.1		
Total		94	100.0		

On why employees had not been trained to regard information security policies as the main tool for achievement of information security management activities, majority (57%) of the respondents claimed training is not their core business, 29% said training is not taken seriously, while few (14%) claimed lack of knowledge to train, as shown in figure 4.5. Firms should be aware that security policy training makes the implementation of security easier, because without training security incidents are likely to increase leading to financial losses (Barman, 2002). When this happens, creativity and innovation levels decrease, in turn leading to low entrepreneurial intensity levels. Affected too at this point is technological entrepreneurship, which provides the much needed *trait d'union* between technologies, innovations and markets (Petti & Zhang, 2013). Organizations therefore, particularly the top 100 medium-sized firms, should not underestimate the importance of entrepreneurial training for example, information security training.

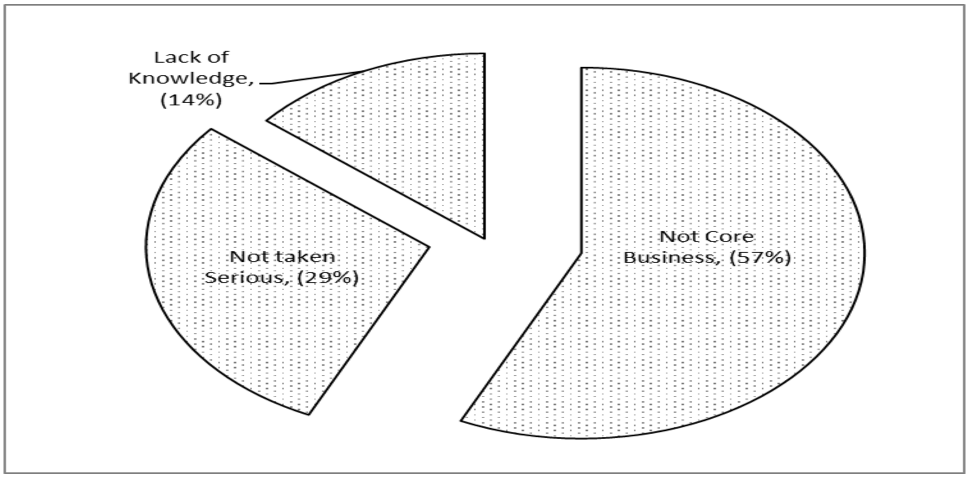


Figure 4.5 Training of Employees

On whether their firms encouraged interdepartmental discussions in regard to updating and improving security policies, majority (84%) of the respondents said yes while a few (14.9%) said no. 1.1% of the respondents did not respond. This is shown in table 4.13. The results show a big percentage of the respondents who indicated that their firms did not encourage interdepartmental discussions in regard to updating and improving security policies. In this regard, firms should consider implementing a comprehensive information security governance framework incorporating, *inter alia*, a process to ensure continued evaluation and updating of security policies (Abu-Musa, 2010). Entrepreneurial motivation is important at this point too, as an important drive that would energize one's actions toward related goals (Dej 2007), and in the current study, towards updating and improving on security policies. Undeniably, policies do align with employees' motivations, perceptions and realities (Renaud & Goucher, 2012). Medium-sized firms should be upfront in creating employee-oriented policies that would in turn create an entrepreneurial culture at firm level thus increasing entrepreneurial intensity levels, in turn leading to better firm performance.

Table 4.13 Interdepartmental Discussions Regarding Updating and Improving Security Policies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	14	14.9	15.1	15.1
	Yes	79	84.0	84.9	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

Respondents were asked why their firms did not encourage interdepartmental discussions in regard to updating and improving security policies, and the majority (50%) of the respondents said interdepartmental discussions are not encouraged in their firms, 25% claimed discussions are not a major concern in their firms, a few (13%) claimed to have a weak IT/ICT department, while another 13% said theirs is a small company which cannot afford the discussions due to limited number of employees. The results are shown in figure 4.6. Stephan and Uhlaner (2010) state that entrepreneurs are embedded in their social environment, such that persons are likely to follow the rules established in their reference groups by restating behavior, either knowingly or unintentionally (Fischer, 2006). This scenario is not surprising because majority of the employees in these firms work on strict deadlines such that time for interdepartmental discussions is quite limited. Thus if a new employee encounters that norm after securing employment in a company, he/she will have a higher incentive to follow suit and is likely to believe that interdepartmental discussions are time wasters and thus not necessary.

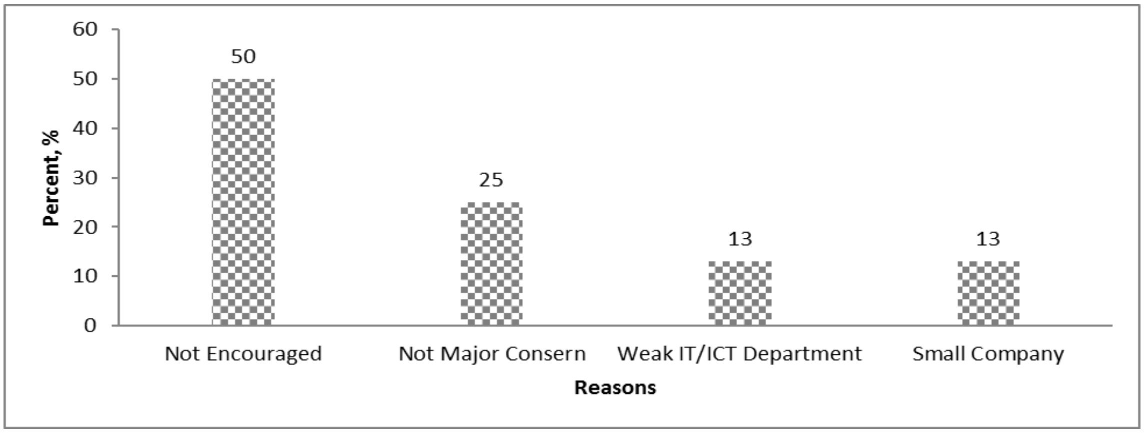


Figure 4.6 Reasons for not Encouraging Interdepartmental Discussions

Measurement of Right Implementation Amongst Medium-sized Firms

Right implementation factor was measured using the Likert scale and the results, expressed as percentages, as shown in table 4.14. The results showed that majority (89.4%) of the respondents agreed with the opinion that information security policies were rightly implemented in such a way that cases of manipulation were unheard of, a few (5.3%) disagreed, while 5.3% were neutral. As Al-Awadi (2009) pointed out, the performance of an organization will be successful if when a policy is created it is rightly implemented, accepted by employees, and the rules followed without manipulating them. This is possible in a firm through behavioral norms produced as a result of following an entrepreneurial culture (Dess & Picken, 1999), emanating as a result of strategic orientation or the strategic directions effected by a firm to create appropriate behaviors for the continuous superior performance of the business (Menguc & Auh, 2005). This often reflects the beliefs and mental models of the firm owners/managers (Hitt et al., 2001). Firm owners/managers of medium sized firms who attempt manipulation would be easily tracked through use of software and therefore, few would attempt manipulation.

On whether an established information security policy review and update process existed in their firms, majority (76.6%) agreed with the opinion, a few (11.7%) disagreed, while another 11.7% remained neutral. The fact that more than 23% of the respondents did not agree with the opinion is a pointer that they were not well versed with the business of security policies. Entrepreneurial training geared towards policy review and update process would reverse this by enabling individuals to both recognize and capitalize on entrepreneurial opportunities (Nichter &

Goldmark, 2009). Majority (87.3%) of the respondents agreed that information security policies in their firms were aligned with business goals, a few (4.2%) disagreed while 8.5% remained neutral. This is in line with the argument of Covin and Slevin (2002) that entrepreneurial leadership is characterized by several imperatives, *inter alia*, protection of innovations threatening the existing business model and making sense of opportunities. This implies that medium-sized firms in Kenya understood their respective business goals in a competitive business environment.

Table 4.14 Response on Right Implementation Factors

Right Implementation Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
ISE1	%	2.1	3.2	5.3	80.9	8.5	3.90	0.673
ISE2	%	2.1	9.6	11.7	72.3	4.3	3.67	0.795
ISE3	%	2.1	2.1	8.5	77.7	9.6	3.90	0.673

Measurement of Acceptance by Employees Factor Amongst Medium-sized Firms

The results of the measurement are shown in table 4.15. The results show that majority (85.1%) of the respondents agreed with the opinion that their firms were successful because upon creation of a policy, it received acceptance by employees, a few (3.2%) disagreed while 11.7% were neutral. This could be attributed to entrepreneurial culture, or a system of shared values and beliefs that shape the firm’s structural arrangements and its members’ actions to produce behavioral norms within an organization (Dess & Picken, 1999). Entrepreneurial culture represents a fertile ground for entrepreneurial activity of employees (Morris, Kuratko & Covin (2008). Further, Morris et al. (2008) gave an overview of characteristics of entrepreneurial culture and mentioned, *inter alia*, the following elements of organizational culture: creation of value through innovation and change, emphasis on essence; hands-on management; commitment and personal responsibility. Of interest in this study is commitment and personal responsibility which could be said to have been exercised by employees of top 100 medium-sized firms, going by the number of respondents who agreed with the opinion.

On whether effective security monitoring was emphasized in their firms in order to enforce security control policies, majority (88.3%) of the respondents agreed, a few (4.2%) disagreed while 7.4% remained neutral. Drucker (2002) avers that information is fundamental to a business and should be protected, and goes on to declare that maintaining the security of information requires effective monitoring and concerted effort by all employees, managers and support staff in a firm. Lack of effective monitoring by medium-sized firms is caused by lack of commitment and personal responsibility (Morris et al., 2008) leading to insecurity. This could result into huge financial losses. Therefore entrepreneurs should enhance security monitoring process.

Table 4.15 Response on Acceptance by Employees Factor

Acceptance by Employees Factors		SD	D	N	A	SA	Mean	Std. Dev.
ISE4	%	2.1	1.1	11.7	77.7	7.4	3.87	0.643
ISE5	%	2.1	2.1	7.4	78.7	9.6	3.91	0.667

Measurement of Teamwork Factor Amongst Medium-sized Firms

Table 4.16 indicates response on teamwork. It shows that majority (92.5%) of the respondents agreed to the opinion that teamwork was encouraged in their firms because to some extent, information security affected everyone, a few (5.3%) disagreed with the opinion while 2.1% remained neutral. This finding contradicts findings by de Lusignan, Chan and Dhoul (2007), who, in their study on The Roles of Policy and Professionalism in the Protection of Processed Clinical Data: A Literature Review, detected a variance between the users and creators of policy. While both parties look for good security, policy writers used taut technical controls over the operation of employees as the main means to this end. This is inappropriate. The ideal situation would be a situation where both the writers and employees work as a team because insecurity affected everyone the same way. Team work increases creativity. Creativity is the basis for innovations and is supported when resources are managed strategically. Innovation is significant to entrepreneurs because it reflects an important means by which firms pursue new opportunities.

On whether information security was a key norm shared by organizational members, majority (89.3%) of the respondents agreed, a few (4.2%) disagreed while 6.4% remained neutral. As Renaud and Goucher (2012) noted in their study, all middle level managers had a responsibility for the security awareness of their staff. Most employees of medium-sized firms saw this as a collaborative effort between training and management. This enhances entrepreneurial culture which allows employees to pursue intrapreneurship. This would lead to an increase in entrepreneurial intensity levels and firm performance. It encourages employees to take risk and be proactive thus making the firm competitive. This is what Top 100 medium-sized firms need, that is, entrepreneurial teams, competitive aggressiveness and proactiveness.

Table 4.16 Response on Teamwork Factor

Teamwork Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
ISE6	%	2.1	3.2	2.1	78.7	13.8	3.99	0.696
ISE7	%	2.1	2.1	6.4	81.9	7.4	3.90	0.640

4.6.3 Analysis of Human-related Information Security Issues

Human-related Information Security Issues were operationalized into culture, awareness and training. When asked whether information security culture was embedded in their organizational culture, majority (92.6%) of the respondents said yes, a few (6.4%) said no while 1.1% did not respond to that question, as shown in table 4.17. In line with this Vroom and von Solms (2004), in their study on Towards Information Security Behavioral Compliance, argued for the development of a security culture within organizations. A firm's culture affects organizational members' expectations of each other as well as their expectations of interactions with stakeholders outside the firm's boundaries, including suppliers and customers. Entrepreneurial culture therefore, being a system of shared values and beliefs, shapes the firm's structural arrangements and its members' actions to produce behavioral norms, that is, the way work is completed in the organization (Dess & Picken, 1999). This is yet another issue which could be attributed to a sound training and awareness programme.

Table 4.17 Whether Information Security Culture was Embedded in Organizational Culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	6	6.4	6.5	6.5
	Yes	87	92.6	93.5	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

On whether their firms use training and awareness programs to enhance and make easier implementation of information security, majority (93.6%) said yes while a few (6.4%) said no, as shown in table 4.18. This contrasts the study by Kimwele et al (2010) where only 28.6% of the respondents were in agreement that their staff received training on IT security. Dhillon (1999) argues that firms must have an ongoing awareness and training programme for employees to deal with the dynamism in the security arena. Entrepreneurship education and training is a major factor in the growth and survival of firms (Njoroge & Gathungu, 2013). It is therefore incumbent upon the Top 100 medium-sized firms to invest in training of employees to ensure survival and growth of their firms.

Table 4.18 Use of Training and Awareness Programs to Enhance and Make Easier Implementation of Information Security

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	6	6.4	6.4	6.4
	Yes	88	93.6	93.6	100.0
	Total	94	100.0	100.0	

The respondents were also asked whether users received adequate security training prior to getting a network account. Majority (92.6%) said yes while a few (7.4%) said no, as shown in table 4.19. Collman and Cooper (2007) contend that while security training is necessary, it is not enough to prevent information security breaches because of individual errors, group failures and system accidents. Patel et al. (2000) on the other hand reiterates that maximum effectiveness is experienced where training is specific to roles and tasks. With adequate security training in place, employees of medium-sized firms can indulge in creativity and innovation without a fear that their innovative ideas could be threatened by insecurity in the system. This would in turn increase entrepreneurial intensity levels in the firms resulting into superior firm performance.

Table 4.19 Whether Users Received Adequate Security Training Prior to Getting Network Account

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	7	7.4	7.4	7.4
	Yes	87	92.6	92.6	100.0
	Total	94	100.0	100.0	

Measurement of Culture Factor Amongst Top 100 Medium-sized Firms

Culture factor was measured using the Likert scale and the results, expressed as percentages, tabulated in table 4.20. The results showed that majority (82.9%) of the respondents agreed to the opinion that their firms made security part of the way they do business, their operational culture, a few (4.2%) disagreed while 12.8% remained neutral. Since entrepreneurial culture shapes the firm's structural arrangements and its members' actions to produce behavioral norms (Dess & Picken, 1999), the firm's culture could be said to affect organizational members' expectations of each other as well as their expectations of relations with stakeholders outside the firm's boundaries.

On whether the influence and guidance of their management fostered a positive attitude of security, majority (85.2%) of the respondents agreed, a few (5.3%) disagreed and 9.6% remained neutral, as shown in table 4.20. Autry and Bobbitt (2008) in their study on Supply Chain Security

Orientation: Conceptual Development and a Proposed Framework, found that the main hindrance was the culture of the employees when it comes to changes in work process. And so they suggested a change to the mindset of each employee so that they start considering security as a personal accountability which could be measured and tracked. Entrepreneurial mindset being a way of thinking about business that focuses on and captures the benefits of uncertainty (McGrath & MacMillan, 2000), organizations capable of successfully dealing with uncertainty tend to outperform those unable to do so (Brorstrom, 2002), and thus an entrepreneurial mindset within medium-sized firms can contribute to a competitive advantage which is necessary for creating wealth.

Table 4.20 Response to Culture Factor

Culture Factors		SD	D	N	A	SA	Mean	Std. Dev.
HRI1	%	2.1	2.1	12.8	75.5	7.4	3.84	0.677
HRI2	%	2.1	3.2	9.6	80.9	4.3	3.82	0.655

Measurement of Awareness Factor Amongst Top 100 Medium-sized Firms

Results of measurement of awareness factor are shown in table 4.21. Majority (88.3%) of the respondents agreed to the opinion that raising security awareness was an important activity that was given an important priority in their firms, a few (6.4%) disagreed with the opinion while 5.3% remained neutral. Smith (2004) in his study on E-security Issues and Policy Development in an Information-Sharing and Networked Environment pointed out that every employee needs a basic awareness of security and its use in order to understand what information needs protection and be held responsible through information ownership.

This was emphasized further in the study by Makumbi, Miriti and Kahonge (2012) who posited that since system users are a common threat to information security, the threat can be addressed by awareness campaigns targeted at the users to sensitize them on security matters. By so doing, an entrepreneurial mindset which is both an individualistic and collective spectacle can be fostered in every employee, enabling them to think and act entrepreneurially and successfully engaging in strategic entrepreneurship. This would also change the mindset of the 6.4% of the respondents who think raising security awareness was an exercise in futility amongst the top 100 medium-sized firms.

Table 4.21 Response to Awareness Factor

HRI Factor		SD	D	N	A	SA	Mean	Std. Dev.
HRI3	%	2.1	4.3	5.3	76.6	11.7	3.91	0.728

Measurement of Training Factor Amongst Top 100 Medium-sized Firms

Results of measurement of training factor are shown in table 4.22. Results show that majority (80.8%) of the respondents agreed to the opinion that to achieve the required outcome from the implementation of an information security, their firms insisted on an on-going regular and structured training and awareness program, a few (6.4%) of the respondents disagreed, while

12.8% were neutral. On whether users received adequate security refresher training appropriate for their job function, majority (79.8%) of the respondents agreed to the opinion, a few (6.4%) disagreed while 13.8% were neutral. Analoui and Samour (2012) in their study on The Managers' Characteristics and their Strategy Development in the Palestinian NGOs: An Empirical Study in Palestine, noted that training is a very important factor in helping managers to improve their managerial skills in general and strategic management skills in particular. To improve managerial competencies and effectiveness by offering the managers chances to attend management training programs would be appropriate, since managers play a crucial role in the success of the business. Strategic orientation or the advantage-seeking behaviors result in superior firm performance.

Table 4.22 Response to Training Factor

Training Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
HRI4	%	2.1	4.3	12.8	73.4	7.4	3.80	0.727
HRI5	%	2.1	4.3	13.8	73.4	6.4	3.78	0.721

4.6.4 Analysis of Information Technology Competence

Information Technology Competence was operationalized into knowledge of information systems, experience in information systems and information systems resources. When asked whether members of staff in their firms had been trained to secure their computers at all times when moving away from their stations, majority (92.6%) of the respondents said yes, a few

(6.4%) responded in the negative, and 1.1% did not respond, as shown in table 4.23. This finding boarders on competence. A study by Fraser, Conner and Yarrow (2003) indicated that desired core competences within organizations, which often depended on effective and creative use of ICT were innovation and agility. Innovation is linked to successful performance for firms in both the industrial and service sectors as well as to entire economies (Kluge, Meffert & Stein, 2000), and effective innovations create new value for customers.

Table 4.23 Trained to Secure Computers at all Times when Moving away from Stations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	6	6.4	6.5	6.5
	Yes	87	92.6	93.5	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

Asked whether members of their staff that traveled with portable computers in their firms were aware of the risk relating to theft and the potential liability through compromised data, majority (96.8%) of the respondents answered in the affirmative while a few (3.2%) said no, as shown in table 4.24. Almost all of them were aware of the risk relating to theft. This was yet another area requiring core competences as was indicated by Fraser et al (2003). A study by Makumbi, Miriti and Kahonge (2012) on An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector found out that loss of computer assets was a prevalent problem within these organizations as no particular measures had been put in place to guard against it.

As indicated by Green, Mitchell and Yarrow (2005), skills and knowledge concerning some key ICT tasks result in sets of core information technology, managerial and organizational competences that could then be leveraged to provide innovation capabilities at the level of the business. On the other hand, resources are the basis of firm differential performances in terms of wealth creation, and resources would enable the top 100 medium-sized firms to engage in strategic entrepreneurship.

Table 4.24 Awareness of the Risk Relating to Theft and Potential Liability Through Compromised Data

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	3	3.2	3.2	3.2
	Yes	91	96.8	96.8	100.0
	Total	94	100.0	100.0	

On whether they were confident that their systems were adequately protected despite being connected to public networks, majority (91.5%) of the respondents answered in the affirmative, a few (7.4%) said no while 1.1% of the respondents were neutral, as shown in table 4.25. Confidence comes with experience in technology. Experience is a distinctive competence that helps companies obtain a competitive advantage (Ong & Ismail, 2008). They propose that experience be assessed by measuring both the diversity of experience (i.e. breadth) and the level of responsibility taken (i.e., intensity). This is illustrative of the level of responsibility required in the top 100 medium-sized firms in ensuring security of their computer systems, despite the myriad of threats emanating from public networks.

Table 4.25 Confidence in Systems being Adequately Protected despite Connection to Public Networks

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	7	7.4	7.5	7.5
	Yes	86	91.5	92.5	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

Measurement of Knowledge of Information Systems Factor Amongst Top 100 Medium-sized Firms

Knowledge of information systems factor was measured using the Likert scale and the results, expressed as percentages, tabulated in table 4.26. The results showed that majority (95.8%) of the respondents agreed to the opinion that expertise on information security was available internally, and where not, their firms took to external advice, a few (2.1%) disagreed while 2.1% were neutral. This finding somehow contradicts that by Dojkovski, Lichtenstein & Warren

(2007) who found out that SMEs generally lack funds, expertise, and time to coordinate and manage security activities. But this contradiction is understandable since the current study is dealing with topnotch medium-sized companies who can afford external expertise. A study by Green, Mitchell and Yarrow (2005) on Towards a Framework for Benchmarking ICT Practice, Competence and Performance in Small Firms, agreed with the finding in the current study when they indicated that external IT experts provided an important source of expertise and advice to small firms. On whether their staff knew what to do with information with regard to its storage, usage, archiving, backup and destruction, majority (94.7%) of the respondents agreed to the opinion, 1.1% of the respondents disagreed while 4.3% remained neutral.

A study by Kimwele, Mwangi & Kimani (2010) on Adoption of Information Technology Security: Case Study of Kenyan Small and Medium Enterprises (SMEs) found out that 76.2% of the respondents had suffered information security breaches within the last 12 months, one of the breaches being backup failure. This is an indication of serious lack of understanding on how to safeguard vital proprietary information. On a positive note, Makumbi, Miriti and Kahonge (2012) found that most of the SMEs used firewalls to guard against hacking, a nevertheless commendable practice but not enough to secure computers at all times as security extends to activities that firewalls cannot guard against, *inter alia*, locking and logging off computers when moving away from one's work station. To overcome this hurdle, an entrepreneurial culture as well as entrepreneurial leadership would be required in the top 100 medium-sized firms. Entrepreneurial culture would shape the firm's members actions to produce behavioral norms

(Dess & Picken, 1999) such that employees are aware of what to do with information, and an entrepreneurial leader would influence other employees to manage resources strategically (Covin & Slevin, 2002), in turn securing computers in the firm as well as the information stored in them.

Table 4.26 Response to Knowledge of Information Systems

Knowledge of Information Systems Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
ITC1	%	2.1	0.0	2.1	68.1	27.7	4.19	0.676
ITC2	%	1.1	0.0	4.3	59.6	35.1	4.28	0.646

Assessment of Experience in Information Systems Factor Amongst Top 100 Medium-sized Firms

Experience in information systems factor was measured using the Likert scale and the results, expressed as percentages, tabulated in table 4.27. The results showed that majority (63.8%) of the respondents agreed that all their systems provided audit trails, a few (13.9%) disagreed while 22.3% were neutral. On whether the roles and responsibilities for information security in their firms were well defined, majority (90.4%) of the respondents agreed, a few (5.3%) disagreed and 4.3% remained neutral. On whether they were confident of technological competence invested in their team over time, majority (91.5%) of the respondents agreed, a few (3.2%) disagreed while 5.3% remained neutral.

As pointed out earlier, these are desired core competences which depended on effective and creative use of ICT (Fraser et al., 2003). Medium-sized firms must be creative to develop innovation. Innovation is significant to entrepreneurs as it is a means by which firms pursue new opportunities. The top 100 medium-sized firms in Kenya that vigorously encouraged innovation are better performers than those that tended to discourage innovation. They should particularly be encouraged to pursue disruptive innovations in order to introduce new ways of playing the competitive game.

Table 4.27 Response to Experience in Information Systems

Experience in Information Systems Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
ITC3	%	1.1	12.8	22.3	53.2	10.6	3.60	0.884
ITC4	%	2.1	3.2	4.3	69.1	21.3	4.04	0.761
ITC5	%	1.1	2.1	5.3	59.6	31.9	4.19	0.723

Measurement of Information Systems Resources Factor Amongst Top 100 Medium-sized Firms

Experience in information systems factor was measured using the Likert scale and the results, expressed as percentages, tabulated in table 4.28. The results showed that majority (87.3%) of the respondents agreed that information systems resources in their firms were adequate, well maintained, and/or replaced as appropriate, a few (3.2%) disagreed while 9.6% remained neutral.

On whether information systems resources were in synchronization with technological advancements, majority (71.2%) of the respondents agreed, a few (6.4%) disagreed while 22.3% remained neutral. This is in line with Prahalad and Hamel's (1990) concept of core competence, where core competence is seen as the capability of the entire organization to learn and to include all firm-specific assets, knowledge and skills and capabilities embedded in the organization, based on technology, processes, structure, and interpersonal and inter group relations. Based on this therefore, the adequacy of information systems resources in a firm as well as technological advancements of assets used, would be satisfactorily taken care of, given the adoption of the concept within the firm. The adoption of the concept in the top 100 medium-sized firms would, in turn, be expected to raise the entrepreneurial intensity levels, culminating into superior performance of the firms.

Table 4.28 Response to Information Systems Resources

Information Systems Resources Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
ITC6	%	1.1	2.1	9.6	71.3	16.0	3.99	0.664
ITC7	%	1.1	5.3	22.3	63.8	7.4	3.71	0.728

4.6.5 Analysis of Information Security Risk Assessment

Information security risk assessment was operationalized into threats and vulnerabilities, potential impact and likelihood of occurrence. When asked whether risk assessment in their firms determine what consequences would be if the infrastructure became inoperable, majority (95.7%) of the respondents answered in the affirmative while a few (4.3%) said no, as shown in table 4.29. Absence of a risk assessment process or one that is inadequate, can lead to severe adverse consequences for firms, *inter alia,* reputation, legal issues or financial loss (Shedden, Scheepers, Smith & Ahmad, 2011). These are the same consequences that would be met if the infrastructure became inoperable. If this happens, many medium-sized firms would experience low entrepreneurial intensity levels, culminating into closure.

Table 4.29 Consequences if Infrastructure Became Inoperable

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	4	4.3	4.3	4.3
	Yes	90	95.7	95.7	100.0
	Total	94	100.0	100.0	

On whether risk assessment in their organizations considered what information assets were subject to laws and regulations and whether the assessment results were adequate in procedure to assure compliance, majority (89.4%) answered in the affirmative while a few (10.6%) said no, as shown in table 4.30. Being a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program (ITGI, 2006), information security governance would guide firms on what information assets were subject to laws and regulations.

Information security governance could help in making certain that organizations are complying with not only applicable laws and regulations, but also codes of practice (von Solms, 2005). This makes it easy for medium-sized firms to adopt best practices as a way of enhancing strategic entrepreneurship. Hitt, Ireland, Camp and Sexton (2001) in their study on Guest Editors' Introduction to the Special Issue Strategic Entrepreneurship: Entrepreneurial Strategies for Wealth Creation, urged firms to have a strategic perspective in their operational processes. Lumpkin and Dess (1996) examined the management processes resulting in entrepreneurial activity, and identified the underlying elements which influenced and enhanced such action. In particular, they introduced the notion of entrepreneurial orientation as a specific concept at the connection between strategy and entrepreneurship and presented this as the right approach.

Table 4.30 Risk Assessment and Information Assets Subject to Laws and Regulations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	10	10.6	10.6	10.6
	Yes	84	89.4	89.4	100.0
	Total	94	100.0	100.0	

On whether medium-sized firms made security and risk assessment part of the way they do business, majority (93.6%) answered in the affirmative, a few (5.3%) said no while 1.1% did not respond, as shown in table 4.31. Information security should not be regarded as a technical issue, but a business and governance challenge that involves adequate risk management, reporting, and accountability (Abu-Musa, 2010). It seems medium-sized firms were leading in this going by the high percentage of affirmative respondents. This finding contradicts an earlier one by Dojkovski, Lichtenstein and Warren (2007) who pointed out that SMEs generally have a weak understanding of information security, security technologies and control measures, and neglect to carry out risk assessment. Top 100 medium-sized firms in Kenya should make security and risk assessment part of the way they do business. This in itself is an entrepreneurial activity with a strategic perspective. This undoubtedly refers to strategic entrepreneurship which involves simultaneous opportunity-seeking and advantage-seeking behaviors (entrepreneurial orientation and strategic orientation respectively) and results in superior firm performance (Ireland et al., 2003).

Table 4.31 Security and Risk Assessment Part of the way Business is Done

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	5	5.3	5.4	5.4
	Yes	88	93.6	94.6	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

Measurement of Threats & Vulnerabilities Factor Amongst Top 100 Medium-sized Firms

Threats and vulnerabilities factor was measured using the Likert scale and the results, expressed as percentages, tabulated in table 4.32. The results showed that majority (98.9%) of the respondents agreed to the opinion that their organization had in place an adequate risk assessment process and a few (1.1%) disagreed. Shedden et al. (2011) states that an inadequate risk assessment process could lead to severe adverse consequences for organizations including financial losses. Resources, including financial capital, are the basis of firm differential performances in terms of wealth creation. The response was one of the highest indicating the severity of non-conformance.

On whether their organizations employed one of the popular ISRA methodologies, majority (96.8%) of the respondents agreed to the opinion, a few (1.1%) disagreed while 2.1% remained neutral as shown in table 4.32. Dhillon (2007), posited that irrespective of the methodology employed by a firm, they generally start with context establishment, followed by risk identification and finally risk analysis. Dhillon in his study had identified a number of methodologies including CRAMM. On whether their staff were trained towards mitigating threats and vulnerabilities, majority (86.2%) of the respondents agreed, a few (2.2%) disagreed while 11.7% remained neutral. Al-Awadi (2009) emphasized that training enhances implementation of information security and make the implementation of security easier. Due to the dynamic nature of information technology training should be carried out in a continuous process in all firms. This is likely to raise the degree of entrepreneurship, leading to superior performance of medium-sized firms.

Table 4.32 Response to Threats and Vulnerabilities

Threats and Vulnerabilities Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
RSR1	%	1.1	0.0	0.0	72.3	26.6	4.23	0.557
RSR2	%	1.1	0.0	2.1	71.3	25.5	4.20	0.579
RSR3	%	1.1	1.1	11.7	62.8	23.4	4.06	0.700

Measurement of Potential Impact Factor Amongst Top 100 Medium-sized Firms

Potential impact factor was measured using the Likert scale and the results tabulated in table 4.33. The results showed that majority (89.3%) of the respondents agreed to the opinion that their firms rated each risk according to potential impact, a few (1.1%) disagreed while 9.6% remained neutral. Rating of potential impact starts with the firm’s most critical information assets followed by the identification of the threats and vulnerabilities of each of these assets (Visintine, 2003).

On whether risk assessment in their firms covered the consequences of a security incident in terms of lost revenues, lost customers and investor confidence, majority (92.5%) of the respondents agreed, a few (1.1%) disagreed while 6.4% were neutral as shown in table 4.33.

Shedden et al (2011) emphasized on this, and stated that any assessment falling short of this would be inadequate. Inadequate risk assessment could lead to severe adverse consequences for organizations including financial losses. The same consequences would be faced if firms failed to rate each risk according to potential impact. At this point no new innovative ideas would be forthcoming and the firm is likely to face closure.

Table 4.33 Response to Potential Impact

Potential Impact								
Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
RSR4	%	1.1	0.0	9.6	70.2	19.1	4.06	0.619
RSR5	%	1.1	0.0	6.4	73.4	19.1	4.10	0.588

Measurement of Likelihood of Occurrence Factor Amongst Top 100 Medium-sized Firms

Likelihood of occurrence factor was measured using the Likert scale and the results tabulated in table 4.34. The results showed that majority (84.0%) of the respondents agreed to the opinion that risk assessment in their firms considered whether the entity could continue to operate if critical information became unavailable, compromised or lost, a few (3.2%) disagreed while 12.8% remained neutral. Absence of some critical information would ground operations of a firm to a halt, and so it is incumbent upon the firms to rate and identify the information in question.

On whether their organization rated each risk according to likelihood of occurrence, majority (91.5%) of the respondents agreed, a few (5.3%) disagreed while 3.2% remained neutral. Likelihood of occurrence being one way of rating the criticality of risks is an indication that risks to organizational assets are organized and then prioritized according to criticality for whatever further action (Alberts & Dorofee, 2004). Likelihood of occurrence should be mitigated by carrying out satisfactory information security risk assessment. Repeated occurrences would disrupt creativity and innovation in a firm. When this happens, entrepreneurial intensity levels decrease resulting into firm closure. Same consequences would be suffered if critical information became unavailable in the firm.

Table 4.34 Response to Likelihood of Occurrence

Likelihood of Occurrence Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
RSR6	%	1.1	2.1	12.8	70.2	13.8	3.94	0.669
RSR7	%	3.2	2.1	3.2	78.7	12.8	3.96	0.732

4.6.6 Analysis of Entrepreneurial Orientation

The constructs that were used to operationalize entrepreneurial orientation were innovativeness, proactiveness and risk taking. When asked whether their firms re-engineered their processes to make them more efficient than their competitors' processes, majority (94.7%) of the respondents answered in the affirmative, a few (3.2%) answered in the negative while 2.1% did not respond, as shown in table 4.35. A study by Kusumawardhani (2013) on The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java, had majority (68.2%) of respondents answer in the affirmative when a similar question was posed to them. This is a demonstration of the level of creativity in a firm. Creativity is very vital in a firm. Indeed as Flynn, Doodley and Cormican (2003) underscored, the ability of an organization to grow is reliant on its ability to produce new creative ideas and to exploit them effectively for the long term benefit of their organization. Medium-sized firms in Kenya need to formulate entrepreneurial strategies which will guarantee them superior firm performance.

Table 4.35 Re-engineering Processes to make them more Efficient than Competitors' Processes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	3	3.2	3.3	3.3
	Yes	89	94.7	96.7	100.0
	Total	92	97.9	100.0	
Missing	System	2	2.1		
Total		94	100.0		

Asked whether their organizations created partnerships with the best partners in the industry before their competitors enlisted them, majority (93.6%) of the respondents answered in the affirmative, a few (5.3%) responded in the negative while 1.1% did not respond, as shown in table 4.36. In a study by Vitale, Giglierano and Miles (2003) on Entrepreneurial Orientation, Market Orientation, and Performance in Established and Startup Firms, majority (64.6%) of respondents answered in the affirmative when a similar question was posed to them.

Partnerships demonstrate open innovation. Small firms have been facing several constraints in differentiating their products and changing their business model. Thus a major liability is that small firms lack the required internal financial resources and technical capabilities (Vanhaverbeke, Vermeersch & de Zutter, 2012). This has necessitated medium-sized firms to collaborate with external partners to innovate successfully, to develop new sources of income, and to reach more profitable positions in the competitive landscape. This is the reason why demand from top 100 medium-sized firms looking to establish or broaden their open innovation initiatives with external sources of innovative ideas has been growing rapidly.

Table 4.36 Creating Partnerships with the best Partners in the Industry Ahead of Competitors

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	5	5.3	5.4	5.4
	Yes	88	93.6	94.6	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

On whether a manager is punished if he/she takes a risk and fails, majority (70.2%) of the respondents answered in the affirmative, a few (27.7%) said no while 2.1% did not respond, as shown in table 4.37. In a study by Kusumawardhani (2013), 44.5% of the respondents answered in the affirmative when a similar question was posed to them. This is indicative of the risk-taking proclivity of a firm, and the results show a higher appetite in the Kusumawardhani study than in the current study. This negates the spirit of entrepreneurship amongst employees of top 100 medium-sized firms. Entrepreneurial environment within a firm matters when it comes to risk propensity. The entrepreneurial environment is also indicative of the rate at which innovative initiatives take place in a firm.

Table 4.37 Punishment after a Manager takes a Risk and Fails

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	No	26	27.7	28.3	28.3
	Yes	66	70.2	71.7	100.0
	Total	92	97.9	100.0	
Missing	System	2	2.1		
Total		94	100.0		

Respondents gave various reasons on being asked whether they would punish their managers when they failed after taking a risk. Majority (44%) of the respondents said they only punished non-risk takers, 38% encouraged calculated risk, 13% said they only punish if a mistake is repeated, even after giving a solution, while a few (6%) responded that risk is part of a business, shown in figure 4.7.

Morris, Lewis and Sexton (1994) posited that economic opportunities arose from organizational innovations whereby entrepreneurs exploit opportunities (inputs) and create new ventures (outputs). Thus, within the framework of the organization, the rate of new product introduction distinguishes entrepreneurial from non-entrepreneurial firms (Drucker, 2002). As well, it is a pointer to entrepreneurial intensity levels in a firm. But this would not happen without taking risks. That is why firms should be discouraged from punishing managers whose risk taking propensity is high.

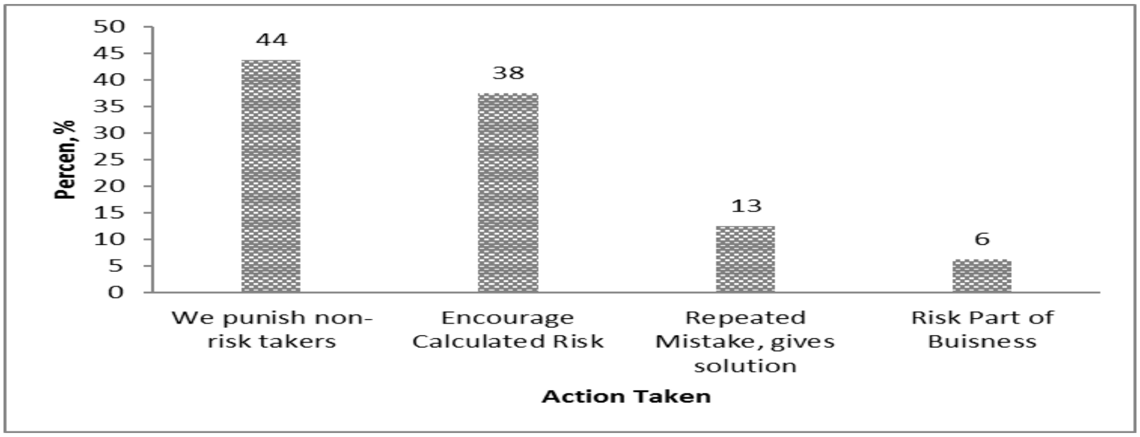


Figure 4.7 Reasons why Punishment not Meted after a Manager takes a Risk and Fails

Measurement of Innovation Factor Amongst Medium-sized Firms

Innovativeness factor was measured using the Likert scale and the results, expressed as percentages, tabulated in table 4.38. The results showed that majority (98.9%) of the respondents agreed to the opinion that their organizations created new products that would provide value to new or their existing customers, while a few (1.1%) disagreed. No respondent remained neutral. This is illustrative of entrepreneurial intensity, which, for any given level of analysis, is a matter of degree, representing a quantitative scale (Heilbrunn, 2008). Economic opportunities emanate from organizational innovations (Morris, Lewis & Sexton, 1994). As a consequence, within the framework of the organization, the rate of new product introduction differentiates entrepreneurial from non-entrepreneurial firms (Drucker, 1985). The higher the rate of new product introduction into the market, the higher the entrepreneurial intensity levels, translating into superior performance of a firm. In a study by Vitale, Giglierano & Miles (2003) on Entrepreneurial Orientation, Market Orientation, and Performance in Established and Startup Firms, majority (65.2%) of respondents answered in the affirmative when a similar question was posed to them.

On whether their firms used non-product ways of creating value for new or existing customers, such as through distribution, advertising or other communications, majority (96.8%) of the respondents agreed to the opinion while a few (1.1%) disagreed. Only 2.1% of the respondents remained neutral. Both scenarios amount to innovation, which refers to the seeking of creative, unusual or novel solutions to problems and needs, with these solutions taking the form of new processes as well as new goods and/or services (Kuratko, Hornsby & Goldsby, 2007). Medium-sized firms must be creative in order to develop innovation, and therefore creativity is progressively important, particularly for firms operating in markets with numerous opportunities to differentiate goods and services (Barney & Arikan, 2001). Top 100 medium-sized firms should understand that, creativity is an incessant process rather than the outcome of single acts and could result in superior firm performance.

Table 4.38 Response to Innovativeness

Innovativeness **Factors**		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
EO1	%	1.1	0.0	0.0	72.3	26.6	4.23	0.557
EO2	%	1.1	0.0	2.1	71.3	25.5	4.20	0.579

Measurement of Proactiveness Factor Amongst Medium-sized Firms

Proactiveness factor was measured using the Likert scale and the results tabulated in table 4.39. When asked whether their firms beat competitors to enter new markets, majority (86.2%) of the respondents agreed to the opinion, a few (2.2%) disagreed while 11.7% remained neutral. Proactivity suggests forward-looking actions where proactive firms anticipates and acts on future requirements by seeking new prospects, introduction of new products and brands into the market ahead of competition (Lumpkin & Dess, 1996).

Proactiveness also shows top management's stance towards encouraging initiatives, competitive aggressiveness, confidence and opportunities in pursuing enhanced competitiveness (Morris, 1998). This could result into increased entrepreneurial intensity levels in top 100 medium-sized firms where future requirements are anticipated and acted upon, and where top management's attitude is positive, translating into improved performance. The results also showed that majority (89.3%) of the respondents agreed to the opinion that their firms introduced new products or services before their competitors did, a few (1.1%) disagreed, while 9.6% remained neutral. Strategic managers managing their firms proactively focus on the future and look for opportunities to exploit for growth, competitive advantage and improved performance (Teece, Pisano & Shuen, 1997). The results suggest that managers of the top 100 medium-sized firms are proactive thus creating competitive advantages by placing the competition in an unenviable position of having to respond to first mover initiatives. Compared to the competition, firms embracing first mover advantage by being the first to produce a new product or service are superior performers.

On whether their firms improved the quality or the number of features of their products or services before their competitors did, and priced them proactively, majority (92.5%) of the respondents agreed to the opinion, a few (1.1%) disagreed while 6.4% remained neutral. Proactiveness is concerned with anticipating and then acting on the premise of a recognized entrepreneurial opportunity (Ireland, Kuratko & Moris, 2006), and therefore firms that exploit opportunities that enable them make first mover initiatives, be the source of competitive advantage and innovation in marketplace battles end up becoming superior performers.

Table 4.39 Response to Proactiveness

Proactiveness Factors		SD	D	N	A	SA	Mean	Std. Dev.
EO3	%	1.1	1.1	11.7	62.8	23.4	4.06	0.700
EO4	%	1.1	0.0	9.6	70.2	19.1	4.06	0.619
EO5	%	1.1	0.0	6.4	73.4	19.1	4.10	0.588

Measurement of Risk Taking Factor Amongst Medium-sized Firms

Risk Taking factor was measured using the Likert scale and the results tabulated in table 4.40. The results showed that majority (84.0%) of the respondents agreed to the opinion that their firms took the risk of missing an opportunity with the same weight as the risk of failure, a few (3.2%) disagreed while 12.8% remained neutral. Risk taking being the willingness to invest resources in business opportunities with possibilities of costly failure (Huang, Wang, Chen & Yien, 2011). Top 100 medium-sized firms pursue opportunities with calculated risks, yielding a robust understanding of potential gains and potential losses that could be associated with decisions to engage in entrepreneurship (Kuratko, Hornsby & Goldsby, 2007). This is the reason why majority of these firms would readily equate the risk of missing an opportunity to the risk of failure, well knowing that if well calculated, the risks are not likely to compromise on their performance.

Asked whether their firms were willing to accept at least a moderate level of risk of significant losses in order to make effective changes to their offering, majority (91.5%) of the respondents agreed to the opinion, a few (5.3%) disagreed while 3.2% remained neutral. Risk-taking involves coming up with new business ventures without the benefit of knowing the probability of success or failure, but with the firm's focus being on identifying and exploiting opportunities in the environment (Shane and Venkataraman, 2000). Top 100 medium-sized firms would mainly venture for new product development, new market segments, new strategic directives, new services or processes, among others, all geared towards superior firm performance.

Table 4.40 Response to Risk Taking

Risk Taking								
Factors		**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
EO6	%	1.1	2.1	12.8	70.2	13.8	3.94	0.669
EO7	%	3.2	2.1	3.2	78.7	12.8	3.96	0.732

4.6.7 Analysis of Firm Performance

Firm performance was operationalized into profitability, return on equity and return on assets. For ease of data collection, these constructs were renamed profitability ratio in the data collection instrument and grouped into five indicators, that is, average pre-tax profits, return on equity, return on assets, employment growth and sales turnover, as shown in table 4.41. The analysis shows the average growth for the indicators of firm performance. From the analysis, the average growth for average pre-tax profits, return on equity, return on assets and employment growth ranged from 90% to 99%, except for the and sales turnover which stood at 125.97%.

A firm's success is mirrored by its tangible resources, in this case its sales turnover. Resource strategy research tries to discover and explain why some firms are more prosperous than others, and is obvious then that strategy is based on resource strengths (Ireland & Hitt, 2005). Ireland and Hitt avers that a firm's resource strengths certainly do provide value creation and contribute to firm performance. This is critical in strategic entrepreneurship. The 2013 top 100 medium-sized firms were successful in this front. Return on assets had the highest amount of variation from the average, an indicator of the varying management efficiency amongst medium-sized firms, at using the assets to generate earnings.

Table 4.41 Firm Performance

FP Factors		Mean	Std. Dev.
PR1	%	96.30	13.17
PR2	%	90.91	9.04
PR3	%	94.07	20.12
PR4	%	99.13	8.46
PR5	%	125.97	8.53

Outliers and Normality Tests of the Study Variables

Outliers were tested univariately on the dependent variable because the dependent variable constructs were in continuous scales. Univariate outliers are extreme values for a single variable (Tabachnick & Fidell, 2007). The results showed possible outliers as indicated in Appendix VI.

This was further evidenced in the testing of normality, as shown in Appendix VII, where the cut-off points for skewness and kurtosis are shown to be outside the -1 and +1 range and more than three times the standard deviation (Kline, 2005).

Testing for Outliers

Outliers within the firm performance constructs were dropped. That is, cases or observations showing characteristics or values that are markedly different from the majority of cases in a data set (Kline, 2005; Hair et al., 2010) are normally dropped. This is because they distort the true relationship between variables, either by creating a correlation that should not exist or suppressing a correlation that should exist (Abbott & McKinney, 2013). Consequently, multivariate testing of outliers on the dependent variable using Mahalanobis d-squared, produced reasonable boxplots as shown in figure 4.8, where all the constructs are symmetrical and with no outliers identified. Multivariate outliers are an unusual combination of scores on a number of variables (Tabachnick & Fidell, 2007).

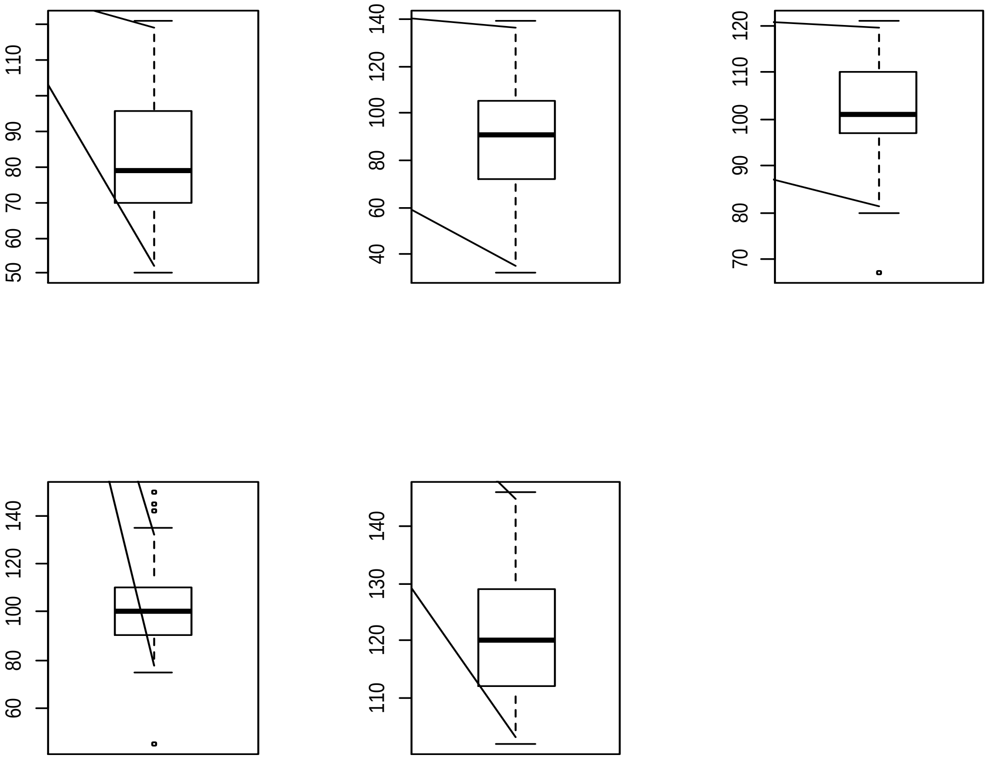


Figure 4.8 Multivariate Testing of Outliers for the Dependent Variable

Testing for Normality

The normality of data distribution was assessed by examining its skewness and kurtosis (Kline, 2005). A variable with an absolute skew-index value greater than 3.0 is extremely skewed while a kurtosis index greater than 8.0 is an extreme kurtosis (Kline, 2005). Cunningham (2008) stated that an index smaller than an absolute value of 2.0 for skewness and an absolute value of 7.0 is the least violation of the assumption of normality. The results of the normality test of the dependent variable indicated skewness and kurtosis in the range of -1 and +1 as shown in table 4.42. This implies that the assumption of normality was satisfied.

Table 4.42 Normality Test of the Dependent Variable

Factor		Statistic	SE (±)
PR1	Mean	85.3	2.0
	Median	79.0	
	Std. Deviation	17.8	
	Range	71.0	
	Skewness	0.5	0.3
	Kurtosis	-0.8	0.5
PR2	Mean	88.9	2.5
	Median	91.0	
	Std. Deviation	22.8	
	Range	107.0	
	Skewness	-0.1	0.3
	Kurtosis	-0.5	0.5
PR3	Mean	101.9	1.2
	Median	101.0	
	Std. Deviation	10.9	
	Range	54.1	
	Skewness	-0.2	0.3
	Kurtosis	0.5	0.5
PR4	Mean	100.2	1.9
	Median	100.0	
	Std. Deviation	17.3	
	Range	105.0	
	Skewness	0.4	0.3
	Kurtosis	-0.3	0.5
PR5	Mean	122.3	1.2
	Median	120.0	
	Std. Deviation	11.0	
	Range	44.0	
	Skewness	0.5	0.3
	Kurtosis	-0.8	0.5

To corroborate the skewness and kurtosis results, the graphical analysis results showed the line representing the actual data distribution closely follow the diagonal in the normal Q-Q plot as shown in figures 4.9 to 4.13, suggesting normal distribution (Hair, Tatham, Anderson & Black, 2006). In q-q plot, or the normal probability plot, the observed value for each score is plotted against the expected value from the normal distribution, where, a sensibly straight line suggests a normal distribution (Pallant, 2007). By and large, if the points in a q-q plot depart from a straight line, then the assumed distribution is called into question (Aas & Haff, 2006).

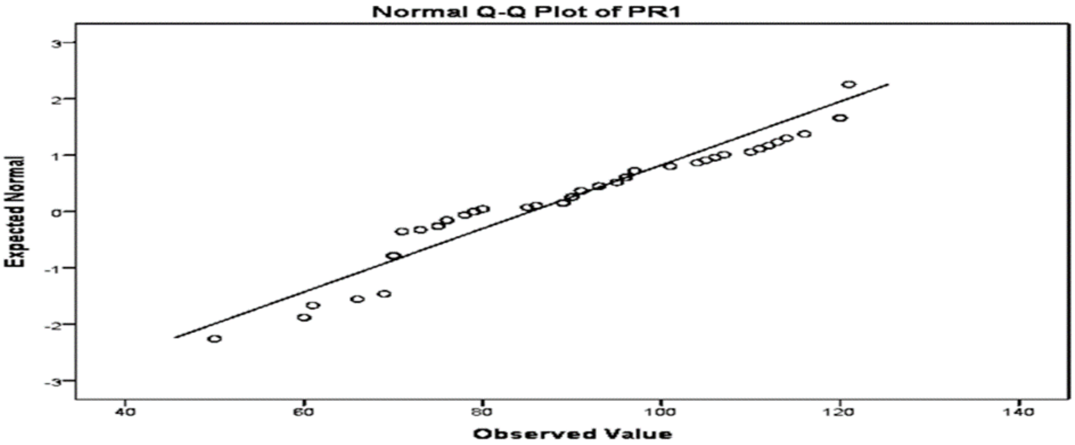


Figure 4.9 Q-Q Plot of Average Pre-tax Profits

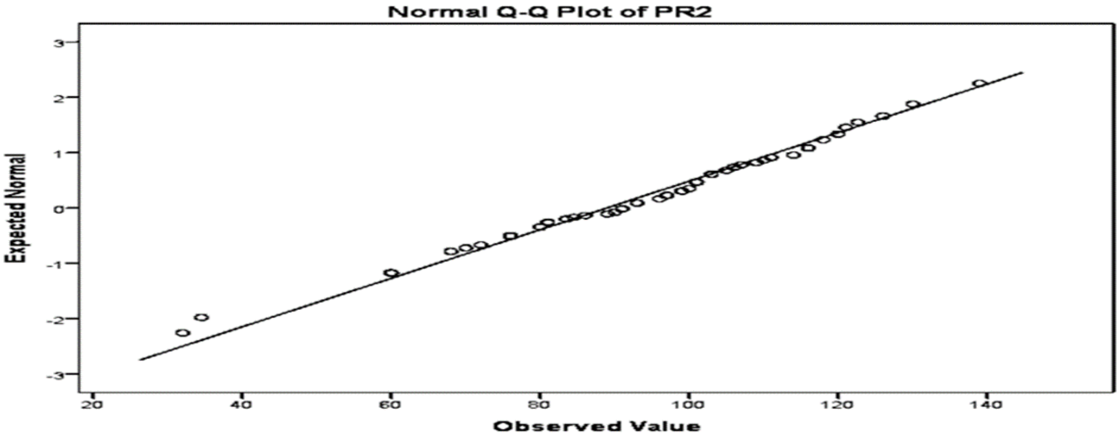


Figure 4.10 Q-Q Plot of Return on Equity

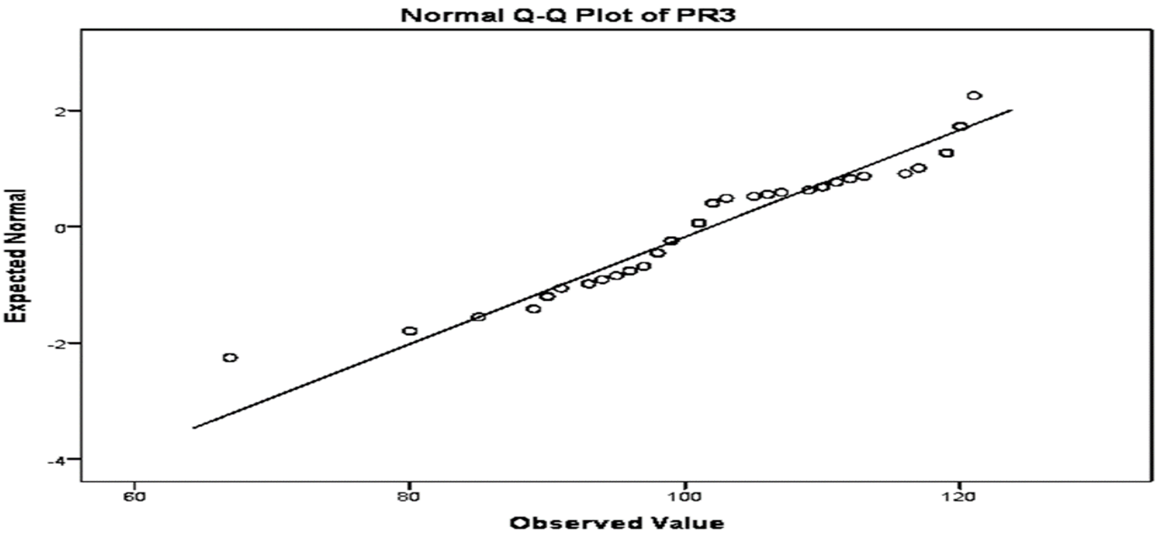


Figure 4.11 Q-Q Plot of Return on Assets

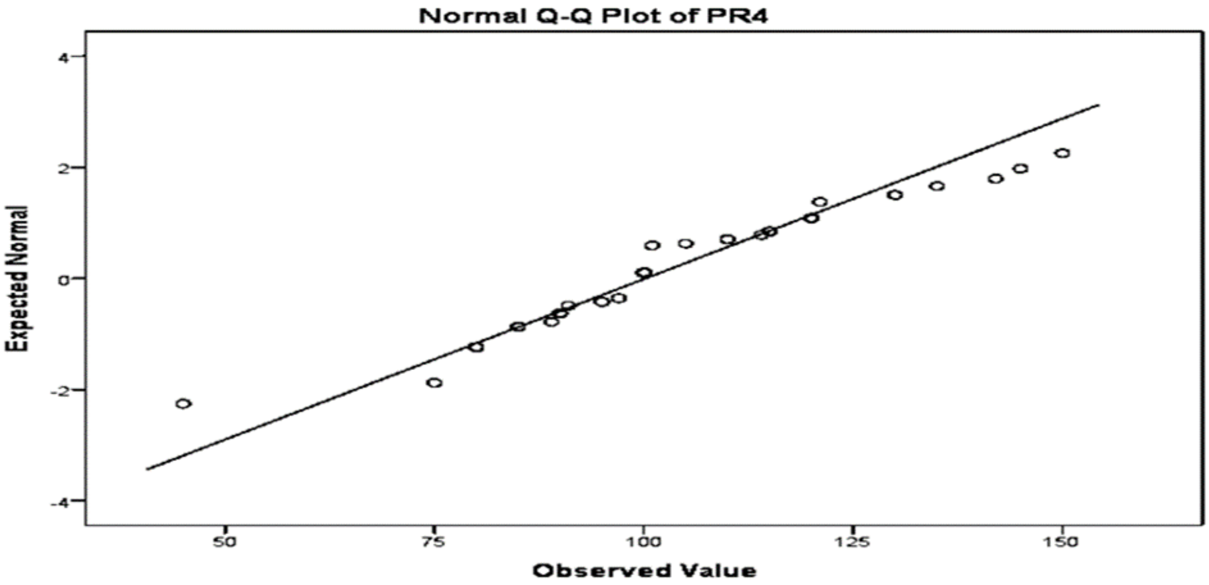


Figure 4.12 Q-Q Plot of Employment Growth

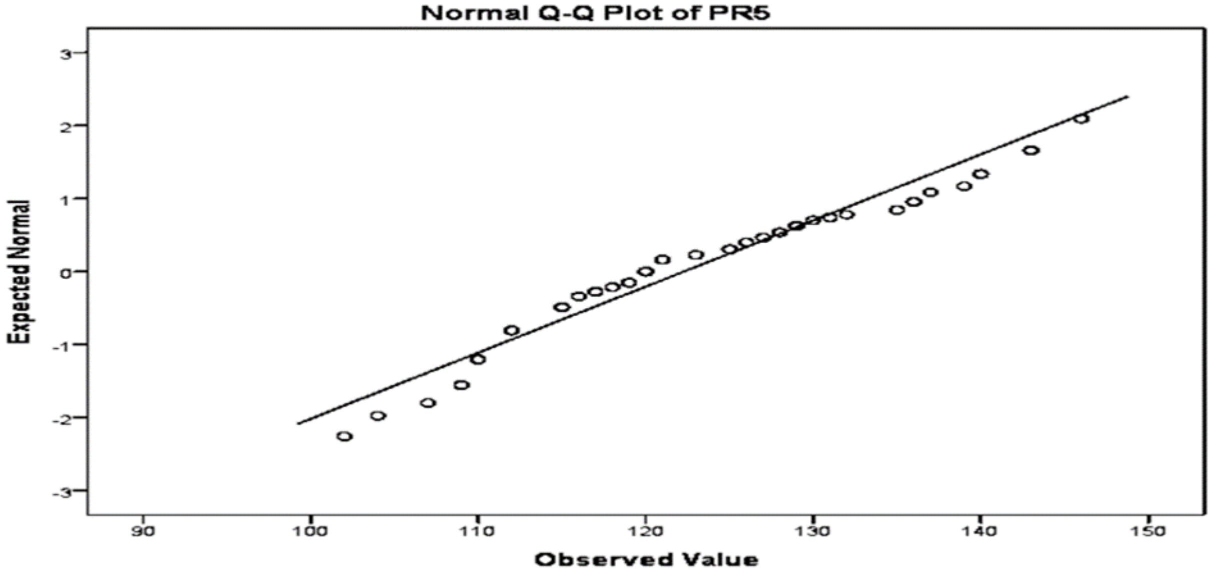


Figure 4.13 Q-Q Plot of Sales Turnover

4.7 Test of Assumptions of the Study Variables

When the assumptions of the linear regression model are correct, ordinary least squares (OLS) provides efficient and unbiased estimates of the parameters (Long & Ervin, 1998). To ensure that there was no violation of the assumptions, this study tested for linearity, homoscedasticity, multicollinearity, non-response bias and common method variance. Prior to embarking on their analysis, Sazali, Haslinda, Jegak, and Raduan (2009) conducted preliminary analyses to ensure that there was no violation of the assumptions of normality, linearity, homoscedasticity, and homogeneity of error variance, in their study on Moderating Effects of MNCs' Size in the Relationship between Degree of Inter-Firm Technology Transfer and Local Firms' Performance. Kim, Kim and French (2014) tested for non-response bias to find out if the answers of the respondents differed from the potential answers of those who did not answer, in their study on What increases firms' performance of information security management and the role of regulatory pressure.

4.7.1 Heteroscedasticity

Heteroscedasticity happens when the variance of the errors varies across observations (Long & Ervin, 1998). When the errors are heteroscedastic, the OLS estimator remains unbiased, but becomes inefficient, and essentially, the usual procedures for hypothesis testing are no longer appropriate. In this study the Breusch-Pagan / Cook-Weisberg test was used to test for heteroscedasticity. Breusch-Pagan / Cook-Weisberg tests the null hypothesis that the error variances are all equal versus the alternative that the error variances are a multiplicative function of one or more variables (Sazali, Haslinda, Jegak & Raduan, 2009). Table 4.43 shows the result of *hettest* by use of the Breusch-Pagan / Cook-Weisberg test. A large chi-square value, greater than 9.21 (Sazali et al., 2009), would indicate that heteroscedasticity was present. In this study, the chi-square value was small, that is, 0.18, indicating heteroscedasticity was not a problem.

Ho: Constant variance

Variables: Top Management Commitment, Information Security Risk Assessment, Human-related Information Security Issues

Table 4.43 Heteroscedasticity Test

Ho	Variables	Chi2(3)	Prob > Chi2
Constant Variance	TMC, ISRA, HRI	0.18	0.7928

4.7.2 Multicollinearity

Multicollinearity is the undesirable situation where the correlations among the independent variables are strong. In other words, multicollinearity misleadingly bloats the standard errors. Thus, it makes some variables statistically insignificant while they should be else significant (Martz, 2013). Tolerance of a respective independent variable is calculated from 1 - R^2. A tolerance with a value close to 1 means there is little multicollinearity, whereas a value close to 0 suggests that multicollinearity may be a threat (Belsley, Kuh & Welsch, 2004). The reciprocal of the tolerance is known as Variance Inflation Factor (VIF). Equally, the VIF measures multicollinearity in the model in such a way that if no two independent variables are correlated, then all the VIF values will be 1, that is, there is no multicollinearity among factors. But if VIF value for one of the variables is around or greater than 5, then there is multicollinearity associated with that variable (Martz, 2013). Table 4.44 indicates the test results for multicollinearity, using both the VIF and tolerance. With VIF values being less than 5, it was concluded that there was no presence of multicollinearity in this study. The VIF shows us how much the variance of the coefficient estimate is being inflated by multicollinearity.

Table 4.44 **Multicollinearity Test Results for the Study Variables**

Variable	**VIF (1/(1-R^2))**	**Tolerance (1-R^2)**
ISRA	2.15	0.4651
EO	1.81	0.5525
TMC	1.60	0.6250
ISPE	2.01	0.4975
ITC	1.73	0.5780
HRI	1.57	0.6369
Mean VIF	**1.81**	

4.7.3 Linearity test

Linearity refers to the consistent slope of change that represents the relationship between an independent variable and a dependent variable. If the relationship between the independent and the dependent variables is radically inconsistent, then structural equation modeling analyses will be difficult to carry out (Mark, 2003). There are several ways of testing for linearity. Perhaps the easiest and clear-cut one, yet rigorous, is the deviation from linearity test. If the significant value for deviation from linearity is less than 0.05, the relationship between independent and dependent variables is not linear, and this presents problems during modeling. Mark also states that issues of linearity can also be fixed by removing outliers. Since this has already been done, we assume linearity of our variables.

4.7.4 Non-Response Bias

This was measured using the extrapolation method of Armstrong and Overton (1977). Out of 94 responses, 83% (n=78) responses were grouped as early responses while 17% (n=16) were grouped as late responses. The evaluation of non-response bias was done by comparing the means of the characteristics of early and late responses. The results of the student test (*t*-test) revealed no significant differences between early and late responses (at p=0.05), providing evidence of a representative and unbiased research sample.

4.7.5 Common Method Variance

When the multi-trait multi-method (MTMM) model heterotrait-monomethod correlations are higher than heterotrait-heteromethod correlations, some portion of the variance in a measure is attributable to the method that was used. This variance is referred to as common method variance (CMV), and it is a form of systematic error variance that can cause observed correlations among variables to differ from their population values (Doty & Glick, 1998). Podsakoff et al. (2003) identified a number of potential sources of CMV organized into four major types, to include sources due to having a common rater, item characteristic effects, item context effects, and measurement context effects, for instance simultaneous measurement of predictor and criterion variables. Since there are a number of ways in which methods can be similar, any of them giving rise to CMV, a questionnaire particularly, might be subject to common method variance.

Rindfleisch, Malter, Ganesan and Moorman (2008) in their study on Cross-Sectional versus Longitudinal Survey Research: Concepts, Findings and Guidelines, gave a threshold of up to 0.21 for the t-statistic value of common method variance test. In this study, the test for the common method variance using CFA marker technique produced a t-statistic of 0.0064 (-0.08^2), as shown in figure 4.14, and thus it was concluded that common method variance was not a concern for this study because of the small figure of less than 0.21. Doty, & Glick (1998) in their study on Common Methods Bias: Does Common Methods Variance Really Bias Results?, tested for common method variance. Podsakoff, MacKenzie, Lee & Podsakoff (2003) in their study on Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, also tested for common method variance, and got a t-statistic of 0.11.

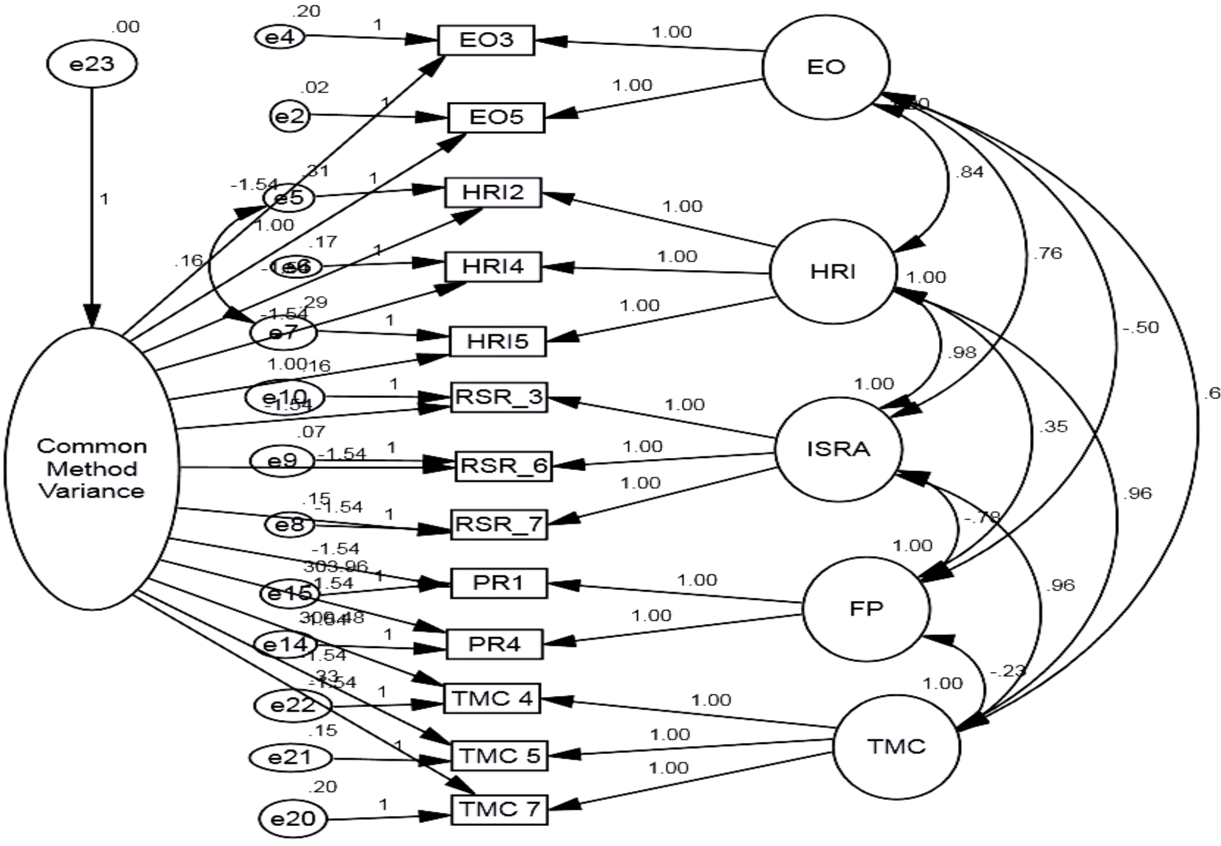


Figure 4.14 Common Method Variance

4.8 Data Analysis and Results of the Study Variables

In this study, data analyses were conducted using a two-phase process consisting of confirmatory measurement model and confirmatory structural model. This is in line with the two-phase process suggested by Anderson and Gerbing (1988). A study on Impacts of organizational capabilities in information security by Hall, Sarkani and Mazzuchi (2011) in their study on Impacts of Organizational Capabilities in Information Security, conducted analyses using a two-phase process consisting of confirmatory measurement model and confirmatory structural model. A study by Kusumawardhani (2013) too on The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java, conducted analyses using a two-phase process suggested by Anderson and Gerbing (1988). Also a study by Latip, Salleh, Omar and Yaakub (2013), on A Resource-based Perspective on Technological Competencies and Relationship Performance: An Empirical Analysis conducted analyses using a two-phase process consisting of confirmatory measurement model and confirmatory structural model.

4.8.1 Confirmatory Measurement Model

The first phase involved confirmatory factor analysis (CFA) that evaluates the measurement model on multiple criteria such as internal reliability, convergent, and discriminant validity. Prior to this was the exploratory factor analysis (EFA) whose key steps included the computation of factor loading matrix, communalities and principal components analysis (PCA).

Exploratory Factor Analysis

Exploratory Factor Analysis (EFA) is used when you have a large set of variables that you want to describe in simpler terms and you have no *a priori* ideas about which variables will cluster together (Tabachnick & Fidell, 2013). Thus EFA is often used at the early stages of research in order to identify the variables that cluster together (Bordens & Abbot, 2014), and provides the researcher with information about the number of factors that best represent the data (Hair, Black & Babin, 2010). The goal of EFA is to identify factors based on data and to maximize the amount of variance explained (Suhr, 2006). The researcher is not required to have any specific hypotheses about how many factors will emerge, and what items or variables these factors will comprise. EFA also does not impose any preconceived structure on the outcome. Hafiz and Shaari (2013) in their study on Confirmatory Factor Analysis (CFA) of First Order Factor Measurement Model-ICT Empowerment in Nigeria used EFA in order to identify the variables that cluster together in their study.

Prior to the EFA, two statistical tests which assess the factorability of data or suitability of data for structure detection were performed, that is, Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity. Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy indicates the proportion of variance in your variables that might be caused by underlying factors, whereby high values (close to 1.0) generally indicate that a factor analysis may be useful with your data (Pallant, 2010). Bartlett's Test of Sphericity tests the hypothesis that one’s correlation matrix is an identity matrix, which would indicate that the variables are unrelated and therefore unsuitable for structure detection. Small values (p < 0.05) of the significance level indicate that a factor analysis may be useful with one’s data. Table 4.45 indicates the results of the test for suitability of structure detection. It is evident that KMO value is 0.871 which is close to 1. This means factor analysis is suitable. With p < 0.05 in the Bartlett's Test of Sphericity, this is an indication of suitability of data for structure detection.

Table 4.45 Results of the test for Suitability of Structure Detection

KMO Measure of Sampling Adequacy	Bartlett's Test of Sphericity	
0.871	Approx. Chi-Square	3349.637
	df	528
	Sig.	***0.000***

A simplified factor loading matrix or a pattern matrix, shown in table 4.46, is a matrix containing the coefficients or "loadings" used to express the item in terms of the factors, that is, interpretation of factors (Rummel, 1970). The more the factors, the lower the pattern coefficients as a rule since there will be more common contributions to variance explained. Rummel further asserts that the pattern matrix loadings are zero when a variable is not involved in a pattern, and close to 1.0 when a variable is almost perfectly related to a factor pattern. In this study, the pattern matrix coefficients ranged from 0.717 to 0.993 thus showing variables are almost perfectly related to a factor pattern. Hall, Sarkani & Mazzuchi (2011) in their study on Impacts of Organizational Capabilities in Information Security, examined factor loadings for each observed variable so that they can identify the correlation of that variable to the underlying construct in order to define the factor structure. This was done before the scales were subjected to confirmatory factor analysis. Kusumawardhani (2013) too on The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java, computed for factor loading matrix in order to define the factor structure.

Table 4.46: Loadings and Cross-Loadings for the Measurement Model

Items	1	2	3	4	5	6	7
ISE6	.961						
TMC 4	.933						
ISE3	.906						
TMC 5	.845						
HRI4	.788						
ITC4	.788						
ISE4	.769						
ISE7	.762						
TMC 7	.717						
EO4		.930					
RSR4		.930					
EO5		.906					
RSR5		.906					
EO3		.876					
RSR3		.876					
ITC2			.958				
HRI2			.958				
HRI5			.790				
ITC5			.790				
HRI3				.975			
ITC3				.975			
EO7					.958		
RSR7					.958		
PR3						.910	
PR1						.901	
PR4							.993

Communality values to measure the variability of each observed variable that could be explained by the extracted factors were checked (Field, 2009). A low value for communality, for instance, less than 0.3, could indicate that the variable does not fit well with other variables in its component, and it is undesirable (Pallant, 2010). Initial communalities are, for correlation analyses, the proportion of variance accounted for in each variable by the rest of the variables. Extraction communalities, on the other hand, as shown in Appendix VIII are estimates of the variance in each variable accounted for by the factors in the factor solution. Small values indicate variables that do not fit well with the factor solution, and should possibly be dropped from the analysis. The extraction communalities for this solution are all greater than 0.7 and are acceptable as this means that the variables fitted well with other variables in their factor (Pallant, 2010). Kusumawardhani (2013) in her study on The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java, checked for communality values to measure the variability of each observed variable, with communality values in her study ranging from 0.542 to 0.785.

The goal of Principal Components Analysis (PCA) is to extract maximum variance from the data set with each component (Tabachnick & Fidell, 2013). The first principal component is the linear combination of observed variables that maximally separates subjects by maximizing the variance of their component scores. The second principal component is the linear combination of observed variables that extracts maximum variability uncorrelated with the first component. The second component is formed from residual correlations. Ensuing components also extract maximum variability from residual correlations and are orthogonal to all previously extracted components, and so there is no redundant information (Singh, 2007). Principal Components Analysis is a method for data reduction, and in PCA, it is assumed that all variability in an item should be used in the analysis (Bhattacharyya, 2011).

Appendix IX on extracted components obtained by constraining factors shows the total variance explained by the initial eigenvalues. This study employed variance percentage, Kaiser's criterion and Scree plot test in order to determine the number of factors that can be best used to represent the interrelations among the set of variables (Hair et al., 2010). Hair et al. further asserts that a factor that accounts for less than 5% of the variance is considered not necessary for further investigation. Kusumawardhani (2013) in her study on The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java, employed the three criteria. Based on these criteria therefore, seven factors, out of a total 45 factors, were imputed. Amongst themselves, they were able to explain 75% of the total variance in the data. The seven factors in the initial solution have eigenvalues greater than 1.5, with the threshold being eigenvalue greater or equal to 1.0 (Hair, Black, & Babin, 2010). The fewer the variables explaining more of the variability in the original variables, the better it is in ensuring that there is no redundant information (Hair et al., 2010).

Appendix IX also shows the variance explained by the extracted factors before rotation. The cumulative variability explained by these seven factors in the extracted solution is 74.88%, showing no difference from the initial eigen values. Thus, nothing of the variation explained by the initial eigenvalues is lost due to latent factors unique to the original variables and variability that simply cannot be explained by the factor model (Hair et al., 2010). Ma, Johnston and Pearson (2008) used PCA to identify key constructs in information security objectives, thereby providing a reduced set of information security management objectives in their study on Information security management objectives and practices: a parsimonious framework.

Confirmatory Factor Analysis

Confirmatory Factor Analysis (CFA), a statistical technique used to verify the factor structure of a set of observed variables, allows the researcher to test the hypothesis that a relationship between observed variables and their underlying latent constructs exists. The researcher uses knowledge of the theory, empirical research, or both, postulates the relationship pattern *a priori* and then tests the hypothesis statistically (Suhr, 2006). Confirmatory Factor Analysis is also frequently used as a first step to assess the proposed measurement model in a structural equation model, and many of the rules of interpretation regarding assessment of model fit and model modification in structural equation modeling apply equally to CFA (Hooper, Coughlan & Mullen, 2008).

Confirmatory Factor Analysis is distinguished from structural equation modeling by the fact that in CFA, there are no directed arrows between latent factors (Schumacker & Lomax, 1996). In other words, while in CFA factors are not presumed to directly cause one another, SEM often does specify particular factors and variables to be causal in nature. In the context of SEM, the

CFA is often called 'the measurement model', while the relations between the latent variables (with directed arrows) are called 'the structural model'. Hafiz and Shaari (2013) in their study on Confirmatory Factor Analysis (CFA) of First Order Factor Measurement Model-ICT Empowerment in Nigeria used the CFA technique to verify the factor structure of a set of observed variables.

Both convergent and discriminant validity are considered subcategories or subtypes of construct validity (Bahl & Wali, 2014). They work together such that if evidence for both convergent and discriminant validity can be demonstrated, then by definition there is evidence for construct validity. But, neither one alone is sufficient for establishing construct validity. For convergent validity, the factor loadings should be 0.5 or higher (Pansuwong, 2009; Hair et al., 2010). But ideally the factor loadings should be 0.7 and above, to guarantee that the construct has convergent validity (Kline, 2005; Hair et al., 2010). In this study, the average loadings are more than 0.7, implying that they are high enough to be convergent, as shown in table 4.46. Therefore, convergent validity is met. To establish discriminant validity, one needs to show that measures that should not be related are, in reality, not related. In table 4.47, none of the loadings is greater than 0.7 (Hair et al., 2010), thus demonstrating discriminant validity.

Table 4.47 Discriminant Validity

Item	1	2	3	4	5	6	7
1	1.000	.289	.583	.340	.314	.110	-.042
2	.289	1.000	.390	.246	.470	.101	.107
3	.583	.390	1.000	.246	.461	.107	-.108
4	.340	.246	.246	1.000	.278	.137	.075
5	.314	.470	.461	.278	1.000	.276	.111
6	.110	.101	.107	.137	.276	1.000	.210
7	-.042	.107	-.108	.075	.111	.210	1.000

Scale reliability was assessed by computing a Cronbach's alpha reliability coefficient for each of the constructs. The average Cronbach's alpha statistic in this study is greater than 0.7, ranging from 0.731 to 0.891, as shown in Appendix X. DeVellis (2003) and Nunnaly and Bernstein (1994) recommended a value of 0.7 and above for the coefficient alpha to infer to the internal consistency of the items. Thus reliability is demonstrated since the overall Cronbach's alpha statistic is greater than 0.7.

Kim, Kim & French (2014) assessed the reliability and validity of the measurement model by evaluating internal consistency (reliability), convergent validity, and discriminant validity in their study on What Increases Firms' Performance of Information Security Management and the Role of Regulatory Pressure. Wali and Bahl (2014), in their study on Perceived Significance of Information Security Governance to Predict the Information Security Service Quality in Software Service Industry: An Empirical Analysis, also assessed the reliability and validity of the measurement model by evaluating internal consistency (reliability), convergent validity, and discriminant validity. Latip, Salleh, Omar and Yaakub (2013) too had all the constructs in their study tested for internal consistency reliability, convergent validity and discriminant validity, in their study on A Resource-based Perspective on Technological Competencies and Relationship Performance: An Empirical Analysis.

Hall, Sarkani and Mazzuchi (2011) estimated their measurement models using confirmatory factor analysis to evaluate the construct internal reliability and validity (convergent and discriminant) prior to simultaneously estimating measurement and structural models. Hafiz and Shaari (2013) too evaluated reliability and validity (convergent and discriminant) in their study on Confirmatory Factor Analysis (CFA) of First Order Factor Measurement Model-ICT Empowerment in Nigeria. In all these studies, the assessments of reliability, convergent validity, and discriminant validity met the respective thresholds.

When an analyst attempts to fit a statistical model to observed data, he or she may wonder how well the model actually reflects the data, that is, the closeness of the observed values to those which would be expected under the fitted model (Arbuckle & Wothke, 1999). One statistical test that addresses this issue is the chi-square goodness of fit test.

This test is commonly used to test association of variables in two-way tables, where the assumed model of independence is evaluated against the observed data. If the computed test statistic is large, then the observed and expected values are not close and the model is a poor fit to the data (Arbuckle & Wothke, 1999). Thus, a non-significant p-value is suitable to indicate that the proposed model fits the observed covariances and correlations adequately (Knapp, 2005). Table 4.48 of this study shows that Chi-square goodness of fit test is significant at p<0.001. Shamsuddin, Othman, Shahadan and Zakaria (2012) used Chi-square goodness-of-fit test in their study on The Dimensions of Corporate Entrepreneurship and the Performance of Established Organization, and got a non-significant p-value.

Table 4.48 Chi-square goodness-of-fit test

Chi-Square	**df**	**Sig.**
866.377	94	.000

4.8.2 Confirmatory Structural Model and Hypotheses Testing of the Study Variables

The second phase involved latent variables structural equation modeling (SEM) to test the hypothesized relationships and to fit the structural model. Structural equation modeling (SEM) is a very general, chiefly linear, chiefly cross-sectional statistical modeling technique (Schumacker & Lomax, 1996). Factor analysis, path analysis and regression all represent special cases of SEM. Structural equation modeling is largely a confirmatory, rather than exploratory, technique, and SEM software is typically used for performing confirmatory factor analysis (Jackson, Gillaspy & Purc-Stephenson, 2009).

In this study, SEM was used to test hypotheses and to fit the theoretical model. A study on Impacts of organizational capabilities in information security by Hall, Sarkani and Mazzuchi (2011) used the structural equation modeling to test hypotheses and to fit the theoretical model. Koong, Merhi & Sun (2013) used structural equation modeling for statistical modeling.

Each model variable was tested for outliers and normality on variables aspects. This was an exploratory data analysis (EDA) for understanding the structure of the variable before further data analyses undertaking. This helped in applying the appropriate analytical data analyses techniques to avoid crucial violations of key assumptions in consequent modeling processes. This was followed by model fit testing. In structural equation modeling, the fit indices establish whether, overall, the model is acceptable, and if acceptable, researchers then establish whether specific paths are significant (Moss, 2009). Scholars such as Marsh, Balla, and Hau (1996), recommend that individuals utilize a range of fit indices. Yet others posit that although χ^2 is the traditional measure used in assessing overall model fit, it tends to be unreliable when sample sizes larger than 200 are used, and so alternative fit indexes could be used as there is no agreement on the best single approach for evaluating model fits (Reinard, 2006; Schumacker & Lomax, 2004). This study, apart from picking on four of the most widely respected and reported fit indices (Hooper et al., 2008), also considered the two types of fit statistics that are commonly used, that is, absolute fit indices and incremental fit indices (Hair et al., 2010). For absolute fit indices, the study picked on Goodness-of-Fit Index, Adjusted Goodness-of-Fit Index and Root-

Mean-Square Error of Approximation, and for incremental fit indices, Comparative Fit Index. This study also examined their interpretive value in assessing model fit.

The Comparative Fit Index (CFI), one of the most popularly reported fit indices due to being one of the measures least effected by sample size, takes into account a sample size that performs well even when sample size is small (Tabachnick & Fidell, 2013). This index assumes that all latent variables are uncorrelated, that is, independent model and compares the sample covariance matrix with this independent model (Kline, 2005). The values for this statistic range between 0.0 and 1.0 with values closer to 1.0 indicating good fit. Indeed, a value of CFI greater than or equal to 0.95 is presently recognized as indicative of good fit (Hu & Bentler, 1999).

Goodness-of-Fit Index (GFI) is used to measure the amount of variance and covariance in the observed correlation matrix that is predicted by the model-implied correlation matrix. Values between 0.90 and 1.0 are indicated acceptable (Arbuckle & Wothke, 1999). Adjusted Goodness-of-Fit Index (AGFI) corrects the GFI, which is affected by the number of indicators of each latent variable. Values for the AGFI also range between 0 and 1.0 and it is generally accepted that values of 0.90 or greater indicate well-fitting models.

Root-Mean-Square Error of Approximation, RMSEA, assesses how poorly the model fits the data by considering the error of approximation, which concerns the lack of fit of the researcher's model to the population covariance matrix. Values up to 0.08 indicate reasonable fit to the data. If the samples are large, values of less than 0.10 are also acceptable (Byrne, 2001). Shamsuddin, Othman, Shahadan and Zakaria (2012) used RMSEA, GFI, CFI, SRMR in their study on The Dimensions of Corporate Entrepreneurship and the Performance of Established Organization.

Influence of Top Management Commitment on Firm Performance in Kenya

The first specific objective of this study was to investigate the influence of top management commitment on firm performance in Kenya. Normality test on the factors produced Skewness values between -1 and +1. The outliers were tested for each of the observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected because the values obtained in testing the model fit indices were within the thresholds as shown in table 4.49.

Table 4.49 Model Fit Indices for the Influence of Top Management Commitment on Firm Performance

Model	CFI	GFI	AGFI	RMSEA
Default model	1.000	.998	.988	.000
Saturated model	1.000	1.000		
Independence model	0.000	.643	.464	.374

The hypothesis to test for this specific objective was:

H_{01}: There is no relationship between top management commitment and firm performance in Kenya.

This study found that there was a positive (regression weight = 1.36) relationship between top management commitment and firm performance, as shown in figure 4.23. In this regard, H_{01} was rejected.

The test for significance for this model is shown in figure 4.15.

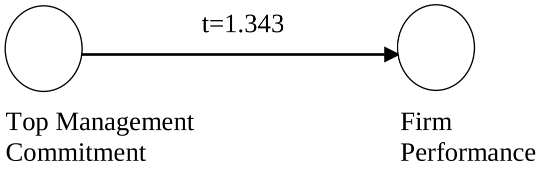


Figure 4.15 Significance Test Result for the Influence of Top Management Commitment on Firm Performance

Therefore this model was significant at 80% significance level (α-level 10% for a 2-tailed test) with t=1.343. Popular α-levels are 10% (0.1), 5% (0.05), 1% (0.01), 0.5% (0.005), and 0.1% (0.001) (Fisher, 1926). The precision is lowered to capture the appropriate significance. In their study on Evaluation of Information Security Management System Success Factors: Case Study of Municipal organization, Kazemi, Khajouei and Nasrabadi (2012) identified top management support as one of the most important success factors in implementing information security management systems, ultimately leading to firm performance. Their findings showed a positive relationship between top management support and information security management. They went on to state that without top management support none of the organizational plans will be implemented. A study by Knapp (2005) on A Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test, found a positive association between top management support and perceived security effectiveness, leading to financial performance of a firm.

Al-Awadi and Renaud (2008) in their study on Success Factors in Information Security Implementations in Organizations found that top management commitment had a relationship with a firm’s information security, leading to firm performance. Their results suggest the right attitude of information security must come from the commitment of top management in order to inspire the rest of the employees to adhere and comply with the organization's security policy rules and regulations. Also a study by Ferrier and Lee (2002) on Strategic Aggressiveness, Variation, and Surprise: How the Sequential Pattern of Competitive Rivalry Influences Stock Market Returns found that information-processing capabilities of a top management team was a significant antecedent of the firm’s competitive behavior.

Firms respond to low performance by implementing strategic changes, which may include the acquisition and development of resources (Greve, 2008). Declining performance influences top management’s strategic choices (Feigenbaum & Thomas, 1988) and compels the management to focus on developing internal resources that may possibly bring a higher return in the future. If performance goals are not realized, firms reexamine their past strategies and eventually adapt or even completely abandon these strategies in an effort to raise performance to the desired levels (Ketchen and Palmer, 1999). But all this is possible with entrepreneurial leadership. In the absence of it, the ability to influence those under you to manage resources strategically in order to emphasize both opportunity-seeking and advantage-seeking behaviors in the firm would come a cropper.

Influence of Information Security Policy Enforcement on Firm Performance in Kenya.

The second objective of this study was to establish the influence of information security policy enforcement on firm performance in Kenya. Normality test on the factors produced Skewness values between -1 and +1. The outliers were tested for each of the observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected. The values obtained in testing the model fit indices were within the thresholds as shown in table 4.50.

Table 4.50 Model Fit Indices for the Influence of Information Security Policy Enforcement on Firm Performance

Model	CFI	GFI	AGFI	RMSEA
Default model	.993	.975	.908	.570
Saturated model	1.000	1.000		
Independence model	.000	.601	.401	.435

The hypothesis to test for this specific objective was:

The second hypothesis of the study was as follows:

H_{02}: There is no relationship between information security policy enforcement and firm performance in Kenya.

As shown in figure 4.23, there was a positive (regression weight = 0.77) relationship between information security policy enforcement and firm performance. Therefore H_{02} was rejected.

The result of test for significance for this model is shown in figure 4.16.

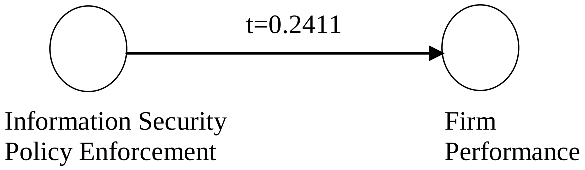


Figure 4.16 Significance Test Result for the Influence of Information Security Policy Enforcement on Firm Performance

Therefore, with t=0.2411, this model was not statistically significant at 80% significance level.

In their study on Evaluation of Information Security Management System Success Factors: Case Study of Municipal organization, Kazemi, Khajouei and Nasrabadi (2012) identified information security policy as one of the most important success factors in implementing information security management systems, consequently leading to firm performance. Their results found a positive relationship between information security policy and information security management. Al-Awadi and Renaud (2008) in their study on Success Factors in Information Security

Implementations in Organizations found that information security policy enforcement had a relationship with a firm's information security leading to improved performance of the firm. Their results advocated a mandatory institution of information security policies to prevent the all rampant cases of unauthorized access to the firm's resources. Also, in their study on What Makes an Effective Information Security Policy?, Hone and Eloff (2002) found that staff who had a greater understanding of security issues and policy development behaved more securely.

However, while this study found a relationship between information security policies and firm performance, this relationship was not statistically significant. A study by Renaud and Goucher (2012) on Health Service Employees and Information Security Policies: An Uneasy Partnership?, revealed that staff often felt restrained by policies, did not get necessary support from top management, and felt pressured to conform and to encourage the staff they managed to act in accordance with policy directives. The study even went to an extent of recommending a recognition and reward scheme to reward secure behavior. This is an indication of high disregard of information security policies by employees, to the extent that firms are forced to create a reward scheme for secure behavior. This behavior can contribute to a decrease in entrepreneurial intensity levels that a firm may have planned to surmount, as some employees would be underperforming awaiting re-assurance of rewards.

Effect of Human-related Information Security Issues (Culture, Awareness and Training) on Firm Performance in Kenya.

The third objective of this study was to explore the effect of human-related information security issues (culture, awareness and training) on firm performance in Kenya. Normality test on the factors produced Skewness values between -1 and +1. The outliers were tested for each of the observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected. The values obtained in testing the model fit indices were within the thresholds as shown in table 4.51.

Table 4.51 Model Fit Indices for the Effect of Human-related Information Security Issues (Culture, Awareness and Training) on Firm Performance

Model	CFI	GFI	AGFI	RMSEA
Default model	.993	.978	.916	.045
Saturated model	1.000	1.000		
Independence model	.000	.673	.509	.336

The hypothesis to test for this specific objective was:

H_{03}: There is no relationship between human-related information security issues and firm performance in Kenya.

Figure 4.23 shows there was a positive (regression weight = 3.01) relationship between human-related information security issues and firm performance. Therefore H_{03} was rejected.

The result of test of significance for this model is shown in figure 4.17.

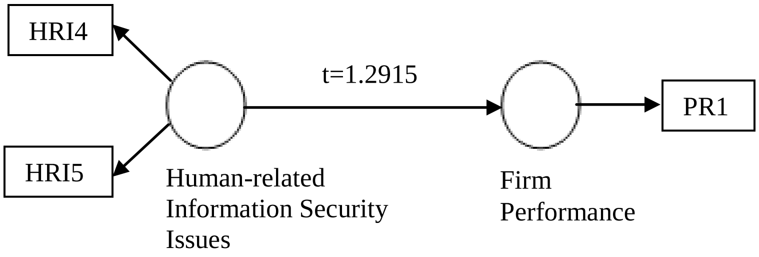


Figure 4.17 Significance Test Result for the Effect of Human-related Information Security Issues (Culture, Awareness and Training) on Firm Performance

Therefore this model was statistically significant at 80% significance level with t=1.295.

In their study on Evaluation of Information Security Management System Success Factors: Case Study of Municipal organization, Kazemi, Khajouei and Nasrabadi (2012) identified both culture and training as two of the important success factors in implementing information security management systems, ultimately leading to firm performance. They found that both culture and training had a positive relationship with information security management. Al-Awadi and Renaud (2008) in their study on Success Factors in Information Security Implementations in Organizations found that awareness and training had a relationship with a firm's information security leading to improved performance of the firm. They stated that with appropriate awareness and security training employees will be made aware of the prevailing security issues including consequences of insecure behavior.

A study by Vroom and von Solms (2004) on Towards Information Security Behavioral Compliance, advocated for the development of a security culture within organizations. Thomson and von Solms (2005) in their study on Information Security Obedience: A Definition, underscored the crucial role played by senior management in cultivating a culture of information security and this was also emphasized by Knapp, Marshall, Rainer and Ford (2006) in their study on Information Security: Management's Effect on Culture and Policy.

A study by Chang and Lin (2007) on Exploring Organizational Culture for Information Security Management, concluded that there were significant relationships between organizational culture and ISM, leading to firm performance. As noted by Melton, Chen and Lin (2006) in their study on Organizational Knowledge and Learning: Leveraging it to Accelerate the Creation of Competitive Advantages, initiatives in conducting business process re-engineering, adopting new information technology, and implementing management or organizational changes normally run into trouble because people do not want to change the culture they are used to. Since entrepreneurial culture is a system of shared values and beliefs that shape the firm's structural arrangements and its members' actions (Dess & Picken, 1999), adoption of a bad culture by employees would result into low firm performance.

As far as training and awareness of information security are concerned, a study by Patel, Arocha and Shortcliffe (2000) on Cognitive Models in Training Health Professionals to Protect Patients' Confidential Information found that maximum effectiveness is scored when security training and awareness are specific to roles and tasks. Hone and Eloff (2002) state that users should be trained in the purpose and functions of security controls. But Collman and Cooper (2007) argue that although security training is necessary, it is not sufficient to prevent information security breaches given individual errors, group failures, and also system accidents which may complicate information security controls. For top 100 medium-sized firms, this is an indicator that it takes more than just training to guard against information security breaches. Breaches in turn result into financial losses for a firm, meaning a downward trend in innovation, and consequently, entrepreneurial intensity levels in their firms.

Influence of Information Technology Competence on Firm Performance in Kenya.

The fourth objective of this study was to assess the influence of information technology competence on firm performance in Kenya. Normality test on the factors produced Skewness values between -1 and +1. The outliers were tested for each of the observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected. The values obtained in testing the model fit indices were within the thresholds as shown in table 4.52.

Table 4.52 Model fit indices for the Influence of Information Technology Competence on Firm Performance

Model	CFI	GFI	AGFI	RMSEA
Default model	.993	.978	.916	.045
Saturated model	1.000	1.000		
Independence model	.000	.673	.509	.336

The hypothesis to test for this specific objective was:

H_{04}: There is no relationship between information technology competence and firm performance in Kenya.

Figure 4.23 shows there was a positive (regression weight = 0.68) relationship between information technology competence and firm performance. Therefore H_{04} was rejected.

The result of test of significance for this model is shown in figure 4.18.

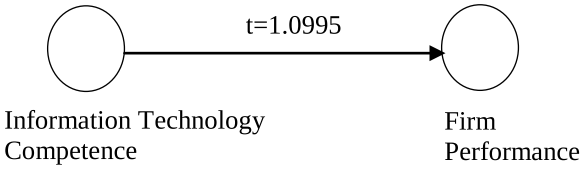


Figure 4.18 Significance Test for the Influence of Information Technology Competence on Firm Performance

With t=1.0995, this study found the model not statistically significant at 80% significance level.

A study by Chang and Ho (2006) on Organizational Factors to the Effectiveness of Implementing Information Security Management found that information technology competence (of business managers) is a determinant of information security management. A study by Arostegui, Benitez-Amado and Tamayo-Torres (2012) on Information Technology-enabled Quality Performance: An Exploratory Study, found a direct effect of IT competence on quality performance improvement. Bacha (2012) in her study on The Impact of Information Systems on the Performance of the Core Competence and Supporting Activities of a Firm found that investing in IS had a significant impact on the performance of the core competence of a firm. A study by Ong and Chen (2013) on Information Technology Capability-Enabled Performance, Future Performance and Value, found a positively significant relationship between firms with superior IT capabilities and superior firm performance. They also found out that IT contributes more to the long-term influences than to the short-term influences.

This is a clear indication of the strategic positioning that IT provides for firms. Certainly, strategic entrepreneurship is an important pathway to value creation (Venkataraman and Sarasvathy, 2001), sustainable competitive advantage (Ireland et al., 2001), and wealth (Ireland et al., 2003), and top managers should pay more attention to the strategic positioning provided to firms by IT rather than the operational effectiveness. Additionally, the desired core competences within organizations which often depend on effective and creative use of ICT are increasing being cited as innovation and agility (Fraser, Conner & Yarrow, 2003).

This is in line with Damanpour and Wischnevsky (2006) observation that the innovative capability of firms to reintroduce their market offers becomes vital to their capacity to survive and grow when they are working under conditions of global competition, rapid technology advances and resource paucity. However, while the current study found a positive relationship between IT competence and firm performance, this relationship was not statistically significant.

This finding corroborates the finding by Ong and Chen (2014) in their study on The effects of IT: from Performance to Value, who found that although IT capabilities positively affected firm performance, the relationship between IT capabilities and firm performance was weak. Thus competence in IT alone in the top 100 medium-sized firms is not enough, but perhaps tempered with some level of creativity and innovation could result into improved firm performance. Top 100 medium-sized firms can enhance technology entrepreneurship, technology innovation and technology management.

Effect of Information Security Risk Assessment on Firm Performance in Kenya

The fifth objective of this study was to determine the effect of information security risk assessment on firm performance in Kenya. Normality test on the factors produced Skewness values of between -1 and +1. The outliers were tested for each of the observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected. The values obtained in testing the model fit indices were within the thresholds as shown in table 4.53.

Table 4.53 Model Fit Indices for the Effect of Information Security Risk Assessment on Firm Performance

Model	CFI	GFI	AGFI	RMSEA
Default model	.993	.978	.916	.050
Saturated model	1.000	1.000		
Independence model	0.000	.673	.509	.412

The hypothesis to test for this specific objective was:

H_{05}: There is no Relationship between Information Security Risk Assessment and Firm Performance in Kenya.

Figure 4.23 shows there was a positive (regression weight = 3.77) relationship between information security risk assessment and firm performance. Therefore, H_{05} was rejected.

The result of test of significance for this model is shown in figure 4.19.

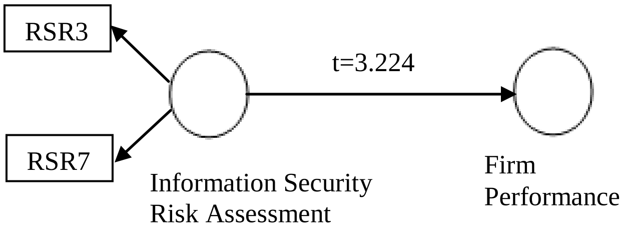


Figure 4.19 Significance Test Result for Effect of Information Security Risk Assessment on Firm Performance

With t=3.224, this model was significant at 95% significance level.

Shedden, Scheepers, Smith and Ahmad (2011) in their study on Incorporating a Knowledge Perspective into Security Risk Assessments found out that information security risk assessment positively influences information security management. Braber, Hogganvik, Lund, Stolen and Vrallsen (2007) in their study on Model-based Security Analysis in Seven Steps - A Guided Tour to the CORAS Method also found that information security risk assessment positively influences information security management. Similar results were obtained by Pattinson and Anderson (2007) in their study on How well are Information Risks being Communicated to your Computer End-Users? A study by Gupta (2011) on Risk Management in Indian Companies: EWRM Concerns and Issues showed that effective risk management can improve organizational performance.

Gupta states that risks are now not perceived as threats (adverse financial effects) but as potential opportunities and goes on to emphasize that enterprise risk management must be perceived and implemented in a strategic way rather than as a routine business function. This is in line with strategic entrepreneurship. Shirokova, Vega and Sokolova (2013) stated that a firm is able to establish and support a balance between opportunity-seeking and advantage-seeking behaviors, which in turn has a positive influence on firm performance, when strategic entrepreneurship is effectively implemented.

While strategic management is focused on seeking advantage, entrepreneurship includes both exploitation of the revealed opportunities and exploration of opportunities (Schindehutte & Morris, 2009). Exploration of opportunities can be achieved through an entrepreneurial orientation (EO) and an entrepreneurial culture (March, 1991). Entrepreneurial culture allows companies to achieve the necessary growth rates and the desired level of competitiveness (Antoncic and Hisrich, 2001), and, combined with entrepreneurial orientation, lead to improved company performance (Covin & Slevin, 1991), and usually with a larger positive effect on performance in hostile environments than in benign ones (Covin & Lumpkin, 2011). Information security management is strategic in positioning top 100 medium-sized firms as entrepreneurial.

In summary, the retained model containing only the sub-variables that were significant after establishing the hypothesized relationships is as shown in figure 4.20. The sub-variables are top management commitment, human-related information security issues and information security risk assessment. Note the average correlations between the sub-variables, with the correlation between ISRA and HRI being the highest.

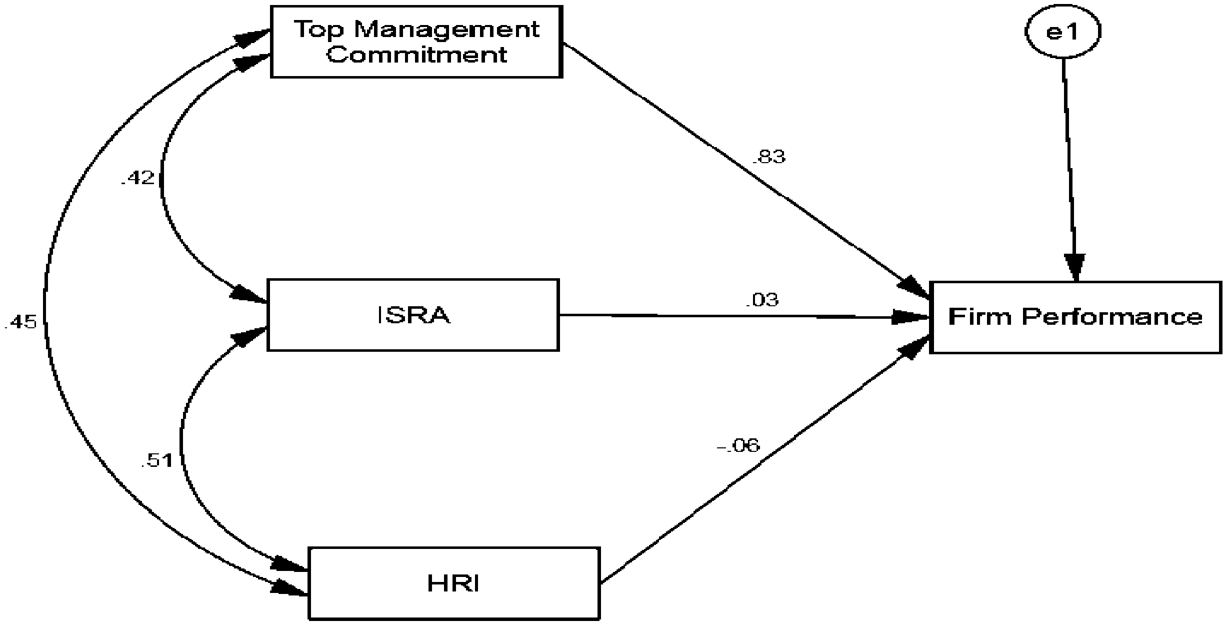


Figure 4.20 The Retained Model after Hypothesis Testing

Effect of Moderation on the Relationship Between Information Security Management and Firm Performance in Kenya.

The sixth objective of this study was to determine whether entrepreneurial orientation moderates the relationship between information security management and firm performance in Kenya. Normality test on the factors produced Skewness values of between -1 and +1. The outliers were tested for each of the observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected. The values obtained in testing the model fit indices were within the thresholds as shown in table 4.54.

Table 4.54: Model Fit Indices for the Effect of Moderation on the Relationship between Information Security Management and Firm Performance

Model	CFI	GFI	AGFI	RMSEA
Default model	.913	.844	.738	.115
Saturated model	1.000	1.000		
Independence model	.000	.291	.173	.326

The confirmatory factor analysis of the full model (with the significant factors only) for this specific objective was as shown in figure 4.21.

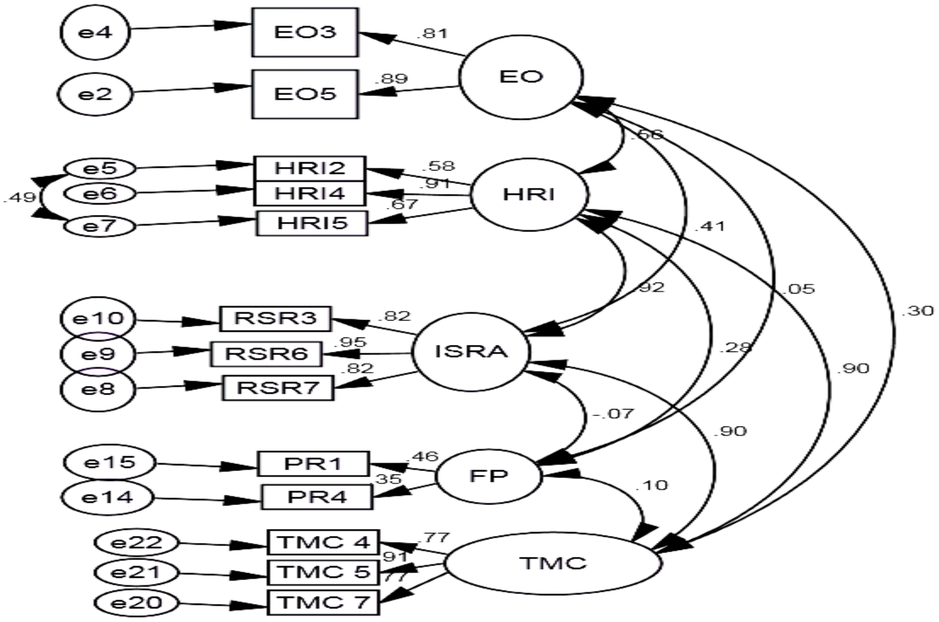


Figure 4.21 Confirmatory factor analysis for the Effect of Moderation on the Relationship between Information Security Management and Firm Performance

The sixth hypothesis of the study was as follows:

H_{06}: Entrepreneurial orientation does not moderate the relationship between information security management and firm performance in Kenya.

Since entrepreneurial orientation moderated the relationship (regression weight = 1.56) between information security management and firm performance, H_{06} was rejected. This is shown in figure 4.23.

The result of test of significance for this model is shown in figure 4.22. With t=1.5001, this model was statistically significant at 80% significance level.

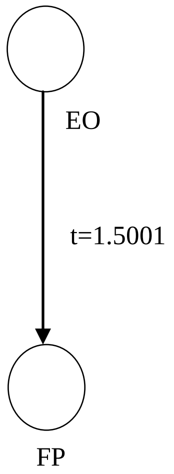


Figure 4.22 Significance Test Result for the Effect of Moderation on the Relationship between Information Security Management and Firm Performance

Although there are a few scholars who have discussed the moderating role of entrepreneurial orientation on the relationship between information security management and firm performance, this study has enriched literature by showing that there is moderation effect, as shown in figure 4.23. Literature, on the other hand, has demonstrated the positive relationship between technological advances and firm performance (Cefis and Ciccarelli, 2005; Roberts, 1999).

Technological entrepreneurship consists of entrepreneurial, managerial and environmental components, and the spirit of the technological entrepreneurship is reflected on a system of collaborative players in activities related to technology development and identification, opportunity recognition, product development, business development and creation (Petti & Zhang, 2011). A study by Siegel and Renko (2012) on The Role of Market and Technological Knowledge in Recognizing Entrepreneurial Opportunities, found that both market knowledge and technological knowledge contribute to firms' subsequent recognition of entrepreneurial opportunities. This is an indication that technological entrepreneurship contributes to a firm's performance.

4.9 Overall Significance Test Results of the Models

Table 4.55 shows the overall significance results of the models. Significance test results for effect of information security policy enforcement on firm performance and significance test results for effect of information technology commitment on firm performance were not significant at 80% significance level. But the rest of the relationships were, with the effect of information security risk assessment on firm performance being significant at 95% significance level. Gordon, Loeb and Zhou (2009) in their study on The Impact of Information Security Breaches: Has There been a Downward Shift in Costs?, tested variables for significance at 5% α level, and if not significant at that level, then at 10% α level, meaning 80% significance level with a 2-tailed test.

Table 4.55: Overall significance results of the models

	Sample Mean (M)	Standard Deviation (STDEV)	Standard Error (STERR)	T Statistics (|O/STERR|)	Conclusion
FP -> EO	0.2251	0.1492	0.1492	1.5001	Significant at 80%
FP -> HRI	0.1725	0.1239	0.1239	1.2915	Significant at 80%
FP -> ISPE	0.0348	0.1428	0.1428	0.2411	Not Significant
FP -> ITC	0.1567	0.1379	0.1379	1.0995	Not Significant
FP -> ISRA	0.247	0.0872	0.0872	3.224	Significant at 95%
FP -> TMC	0.162	0.1209	0.1209	1.343	Significant at 80%

4.10 Overall Structural Equation Model

An overall structural equation model encompassing the measurement models and structural model was established by extending the hypothesized relationships among the latent variables, depicted graphically with straight one-headed arrows as shown in figure 4.23. In the hypothesized relationships, firm performance was set as the dependent variable or endogenous latent variable. Five independent latent variables, that is, top management commitment, information security policy enforcement, human-related information security issues, information technology competence, and information security risk assessment were set as exogenous variables. Entrepreneurial orientation was set as the moderator in the relationship between the endogenous and exogenous variables. The hypothesized structural equation model was tested using the maximum likelihood method and evaluated on the same fit criteria used in assessing the measurement models.

All the regression weights for the variables, except that for Information Security Policy enforcement and Firm Performance relationship at 0.77 and Information Technology Competence and Firm Performance relationship, at 0.68, were significant at the 0.10 α-level indicating reasonable specification of the structural equation model (Schumacker & Lomax, 2004). All alternative fit statistics in Table 4.56 showed acceptable fit threshold levels, suggesting a good fit between the hypothesized model and the data. The model data confirms significant associations in the moderated relationship between information security management and firm performance.

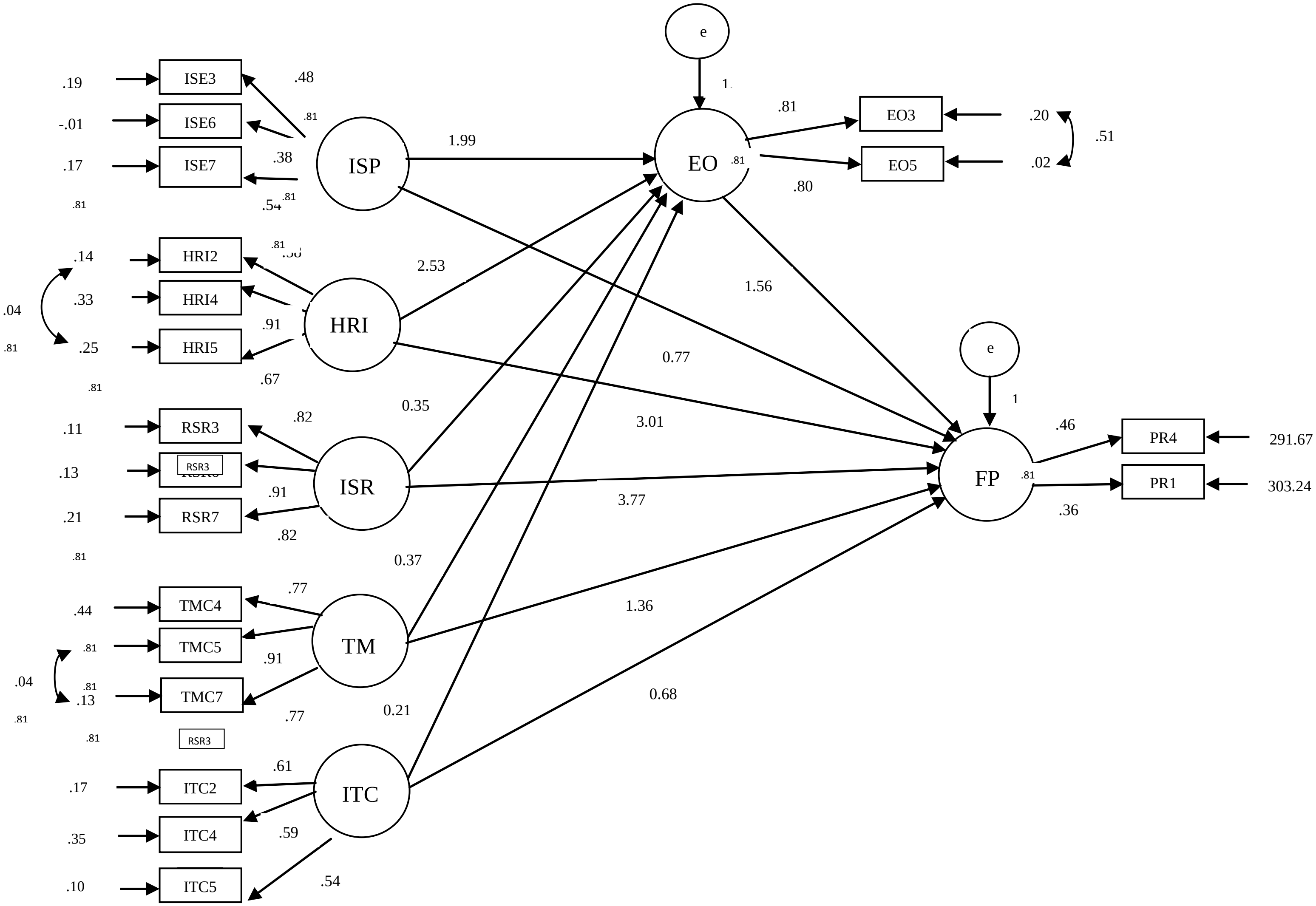


Figure 4.23 Structural Equation Model

Table 4.56 Model Fit Indices for the Overall Structural Model

Model	CFI	GFI	AGFI	RMSEA
Default model	.853	.789	.722	.133
Saturated model	1.000	1.000		
Independence model	.000	.291	.173	.326

4.11 Confirmatory Structural Modeling with Moderation

Structural Equation Modeling (SEM) with moderation was carried out. Prior to moderation, a bootstrapping procedure (Hesterberg, 2003) to evaluate the statistical significance of each path coefficient was carried out, resulting in the initial model in figure 4.24. The t-statistics indicate that Top Management Commitment (TMC) and Information Security Risk Assessment (ISRA) were significant at 10% α level (t-statistics > 0.842). This finding was corroborated during the testing of the hypothesized relationships, where the two factors featured amongst the three that were found to be significant.

In this study therefore, it can be deduced that Top Management Commitment and Information Security Risk Assessment were the most outstanding factors of information security management in the relationship between information security management and firm performance. Bahl and Wali (2014) used a bootstrapping procedure to evaluate the statistical significance of each path coefficient in their study on Perceived Significance of Information Security Governance to Predict the Information Security Service Quality in Software Service Industry: An Empirical

Analysis. The number of bootstrap samples should be 5000 and number of bootstrap cases should be the same as the number of valid observations (Hair, Ringle, & Sarstedt, 2011). Latip, Salleh, Omar and Yaakub (2013), used a bootstrapping procedure with 500 re-samples in their study in order to provide the mean value and the standard deviation for each path model coefficient.

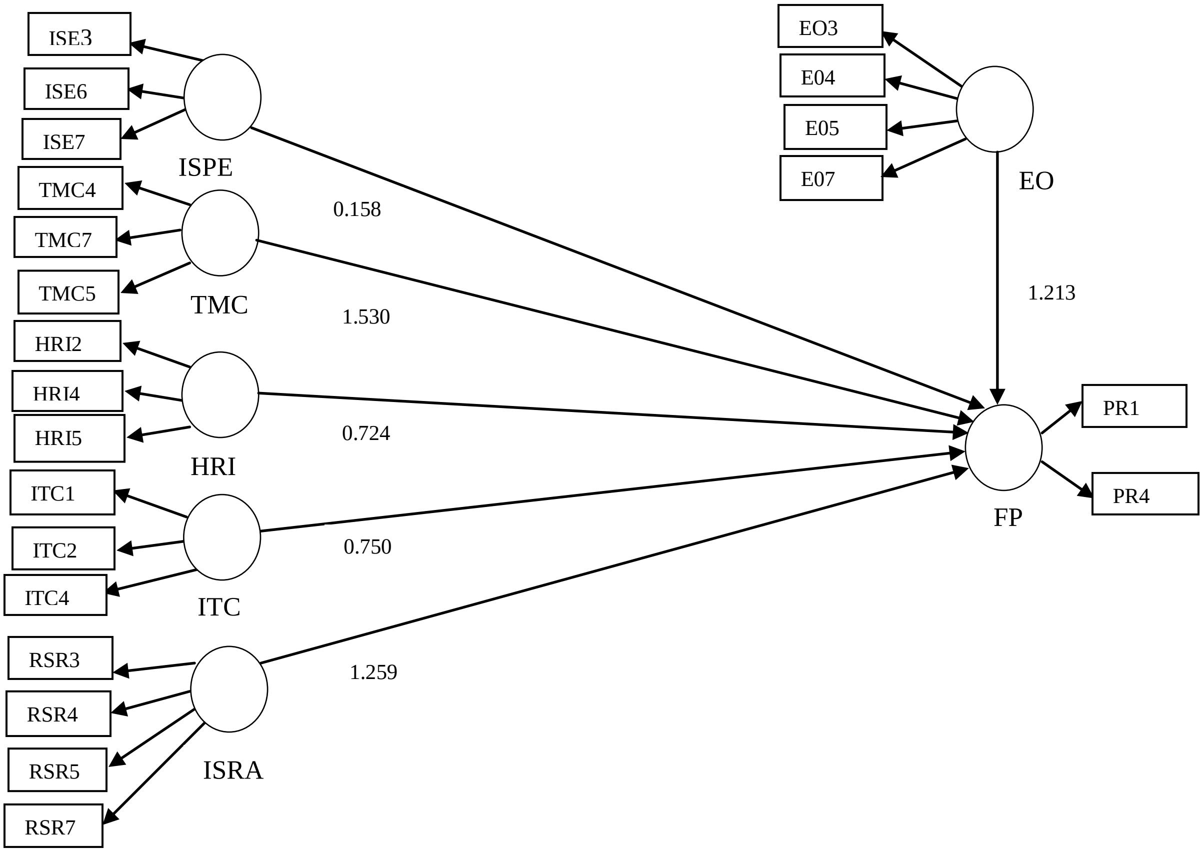


Figure 4.24 Weights Initial Model with Bootstrapping

First Order Construct using the t-statistics through bootstrapping produced significant interactions, ISPE*EO and HRI*EO (t-statistic > 0.842) at 10% α level, as shown in figure 4.25.

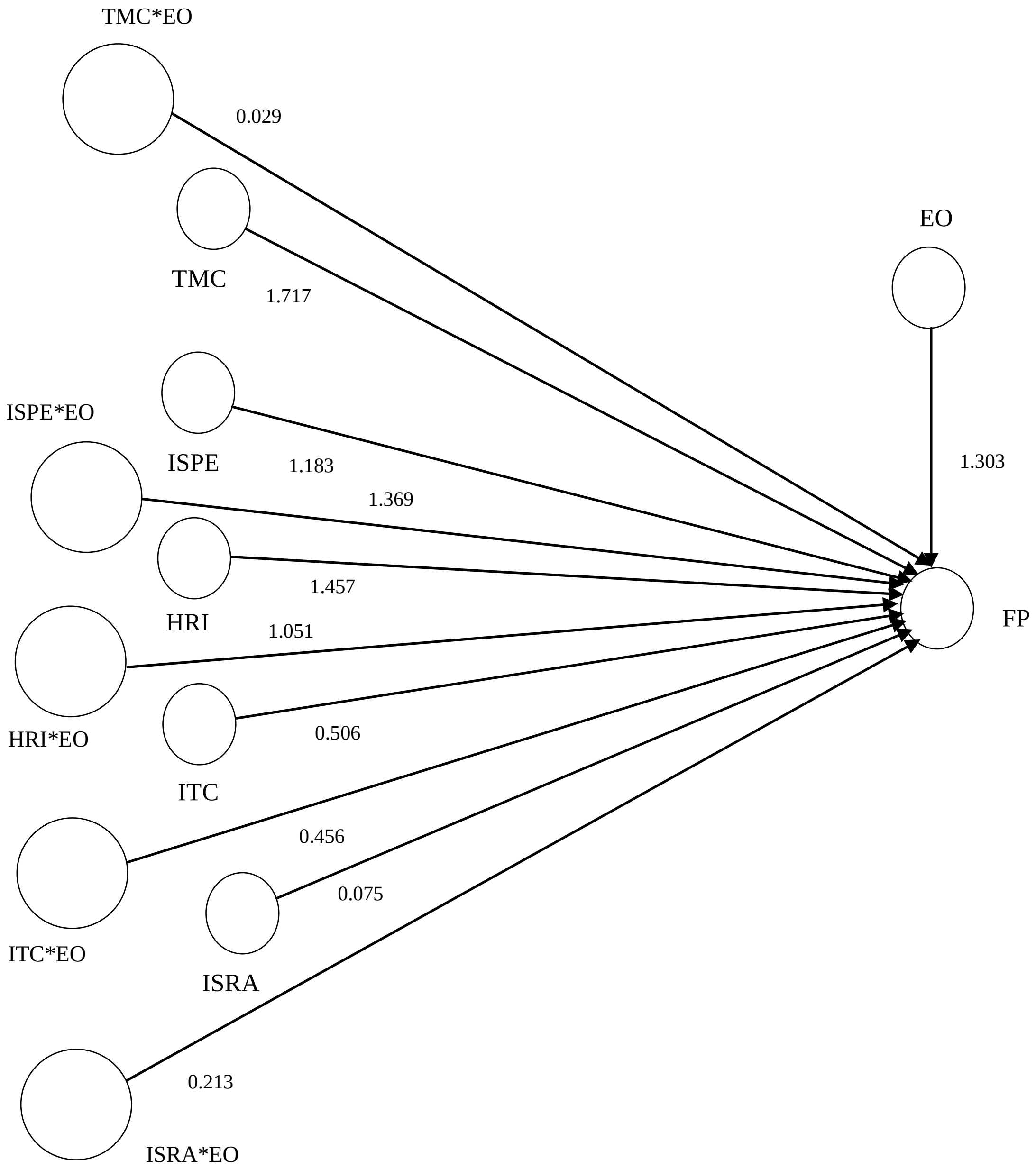


Figure 4.25 First Order Construct

The insignificant interactions, that is, TMC*EO, ITC*EO and ISRA*EO, which had t<0.842 (Fisher, 1926) were dropped and the model re-run. This resulted into a path model analysis for first order construct with only the significant interactions, as shown in figure 4.26. As shown in the figure, the loadings improved with the interaction ISPE*EO improving from t=1.369 to t=1.923. Likewise, the interaction HRI*EO improved from t=1.051 to t=1.087. Thus it can be gathered that dropping of poorly loading interactions and re-running the model improves the statistical significance of the path coefficients.

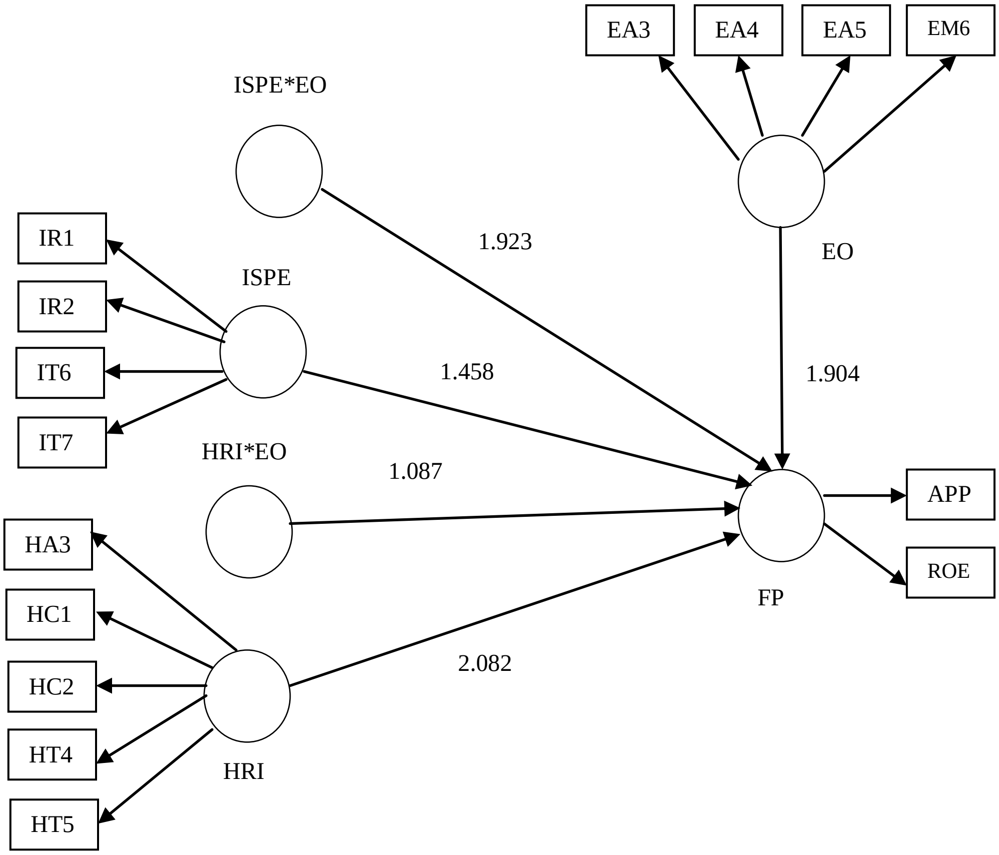


Figure 4.26 Path Analysis with 2 Latent Variables

The next step involved testing the significance for the synergies of the factors at a higher level. This was done at second order level, where TMC, ISPE and HRI factors were grouped together to form Non-technical factor, while ITC and ISRA factors were grouped to form Technical factor. Second-order models are applicable in situations where there is a higher order factor that is hypothesized to account for the relations among the lower order factors (Chen, Sousa & West, 2005). Chen et al., further state that in comparison to first-order models, second-order factor models can provide a more parsimonious and interpretable model when researchers hypothesize that higher order factors underlie their data. This was the case in this study.

When the model was run without interaction terms, the Non-technical and Technical factors showed statistical significance at 5% α level. This contrasts with earlier findings when the first order model was run, where the t-statistics indicated that only top management commitment and information security risk assessment factors were significant at 10% α level. As Rindskopf and Rose (1988) observed, when the first order model fails to provide an acceptable solution, a second-order model can be used to put a structure on the correlations between the first order factors. At this point it can be concluded that at second order model level, all the five variables were positive and statistically significant at 5% α level, an indication that the second order model provided a more acceptable result and also achieves a valid model fit for the collected data.

Chen, Sousa and West (2005) tested for both first order and second order models in their study on Testing Measurement Invariance of Second-Order Factor Models. Bishop and Hertenstein

(2004) also tested for both first order and second order models in their study on A Confirmatory Factor Analysis of the Structure of Temperament Questionnaire. Hafiz and Shaari (2013) in their study on Confirmatory Factor Analysis (CFA) of First Order Factor Measurement Model-ICT Empowerment in Nigeria, too, carried out first order measurement model as a way of testing how well measured variables represent in a small construct. They also carried out second order model analysis to achieve a valid model fit for the data they had obtained as well as theoretical supports behind their developed model. Second order SEM with moderation is demonstrated in figure 4.27.

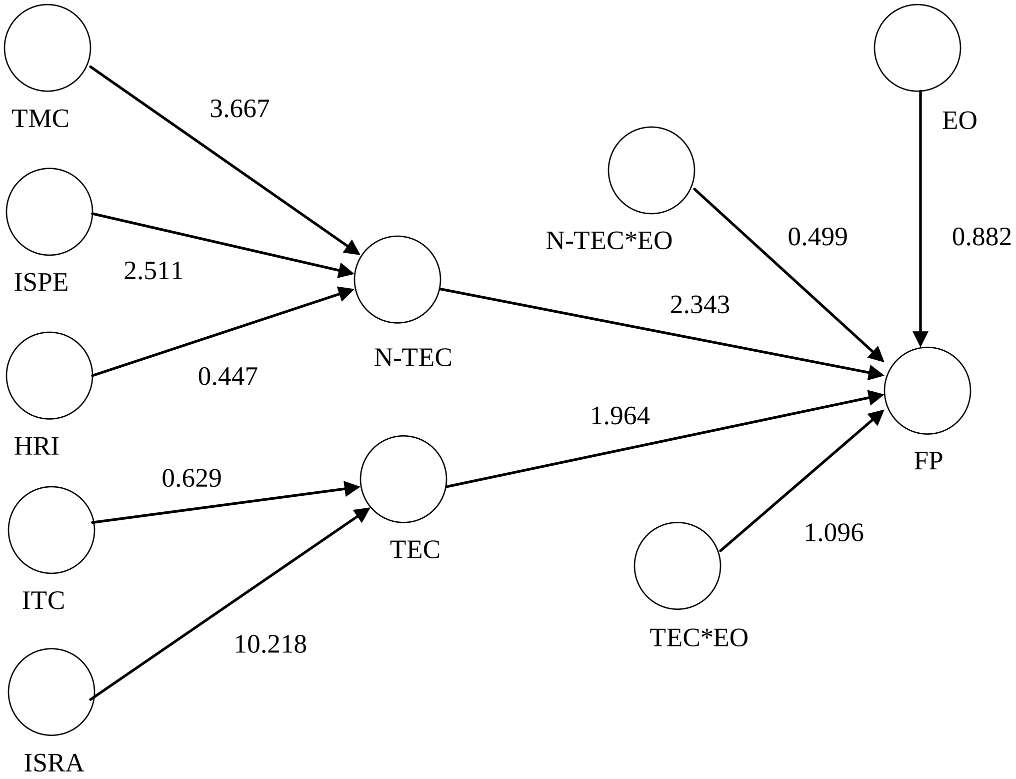


Figure 4.27 Second Order SEM with Moderation

When run with interaction terms on the other hand, the Non-technical*EO interaction was not statistically significant while the Technical*EO interaction was statistically significant at 10% α level. Technical*EO interaction is insightful since this study is also advancing technology entrepreneurship. Technological entrepreneurship is an essential way to commercialize technological innovations, and countries across the world use policy instruments to back technological entrepreneurship (Zhang, Peng & Li, 2008). Technological entrepreneurship activity reflects the extent of commercialization and corporate innovation of an SME (Sui, Sheng & Song, 2005). Top 100 medium-sized firms can strengthen their support for technological innovation in order to enhance their advantage in technological entrepreneurship as emphasized by Sui et al. Thoumrungroje (2003) in her study on Entrepreneurial Intensity, National Culture and the Success of New Product Developments: The Mediating Role of Information Technology, found that entrepreneurial intensity is positively associated with application of Information Technology. The results of this study confirm Thoumrungroje's findings.

The World Economic Forum holds that the management of technology, innovation and information have emerged as key requirements for firm success in the 21st century (Claros, Altinger, Blanke, Drzeniek, & Mia, 2006). Therefore, companies, particularly medium sized businesses need to become more entrepreneurial in order to increase their competitiveness (Antoncic & Hisrich, 2001; Drucker, 2002) and survive and prosper in turbulent business environments (Lumpkin & Dess, 1996). Being more entrepreneurial means increasing entrepreneurial intensity levels (Morris & Sexton, 1996). These two authors tested entrepreneurial intensity empirically as a two-dimensional construct. They argued that entrepreneurial intensity is a function of the degree and frequency of entrepreneurship as shown in figure 4.28 (Morris, 1998). Top 100 medium sized firms in Kenya can allude to this.

Morris (1998) further states that the frequency of entrepreneurship refers to the number of times an enterprise acts entrepreneurially (for example, in developing new products or processes), while the degree of entrepreneurship, similar to EO, is measured by three sub-dimensions: innovativeness, risk-taking, and proactiveness. The fact that entrepreneurial intensity refers to the degree and frequency of entrepreneurship in the organization in a sense represents the strength of the entrepreneurship strategy that exists in that firm (Ireland, Kuratko, & Morris, 2006).

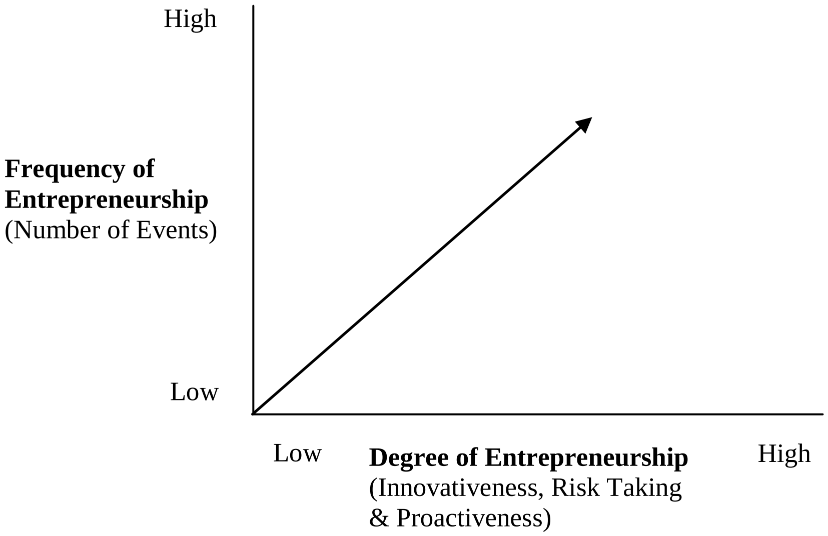

High
Frequency of Entrepreneurship
(Number of Events)
Low
Low
Degree of Entrepreneurship
(Innovativeness, Risk Taking & Proactiveness)
High

Figure 4.28 The Variable Nature of Entrepreneurship

This demonstrates the close association between entrepreneurial orientation and entrepreneurial intensity, and the fact that entrepreneurial orientation and entrepreneurial intensity are complementary, a managerial philosophy top 100 medium sized firms can embrace (Liao, Murphy & Welsch, 2005).

4.12 Moderating Effect of Entrepreneurial Orientation on the Relationship Between Independent and Dependent Variables

Using moderated multiple regression (MMR) analysis in this study, the moderating effect of the variable (interaction term) was analyzed by interpreting the R^2 change in the models obtained from the model summaries, and by interpreting the regression coefficients for the interaction term obtained from the coefficients' tables. Sazali, Haslinda, Jegak & Raduan (2009) used MMR analysis in their study on Moderating Effects of MNCs' Size in the Relationship between Degree of Inter-Firm Technology Transfer and Local Firms' Performance, by analyzing the moderating effect of the variable (interaction term), by interpreting the R^2 change in their models and by interpreting the regressions coefficients for the interaction term.

The results of the moderated multiple regression (MMR) analysis corroborated the results of the Structural Equation Modeling (SEM) with moderation reported earlier in which the first order construct using the t-statistics through bootstrapping produced significant interactions, that is, information security policy enforcement*entrepreneurial orientation on one hand, and human-related information security issues (culture, awareness and training)*entrepreneurial orientation on the other (t-statistic > 0.842), at 10% α level. Sections 4.14.1 and 4.14.2 give the details of the analysis.

4.12.1 Moderating Effect of Entrepreneurial Orientation on the Relationship Between Information Security Policy Enforcement and Firm Performance

Table 4.57 shows the moderating effect of entrepreneurial orientation on the relationship between information security policy enforcement and firm performance. From table 4.57, Model 1 shows that $R = .844$, $R^2 = .712$ and [$F (2, 79) = 97.885$, $p = .0001$]. The value of R^2 indicates that 71.2% of the variance in the Firm Performance can be accounted by Information Security Policy Enforcement scores and Entrepreneurial Orientation. Model 2 in table 4.57, shows the results after the interaction term (Information Security Policy Enforcement*Entrepreneurial Orientation) was added into the model. Table 4.57 also indicates that the inclusion of the interaction term resulted into an R^2 change of .0351, [$F (1, 78) = 4.4763$, $p < 0.10$], showing presence of significant moderating effect. To put it differently, the moderating effect of Entrepreneurial Orientation gained 3.51% variance in the Firm Performance, above and beyond the variance by Information Security Policy Enforcement and Entrepreneurial Orientation. In general, the amount of change in R^2 is a measure of the increase in predictive power of a particular dependent variable or variables, given the dependent variable or variables already in the model (Stockburger, 2001). Thus the null hypothesis was rejected and therefore entrepreneurial orientation moderates the relationship between Information Security Policy Enforcement and Entrepreneurial Orientation.

Table 4.57 Moderated Multiple Regression Model Summary for Information Security Policy Enforcement

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.844[a]	.712	.705	.54294655	.712	97.885	2	79	.000
2	.903[b]	.702	.692	.52643541	.0351	4.4763	1	78	.070

a. Predictors: (Constant), Entrepreneurial Orientation, Information Security Policy Enforcement
b. Predictors: (Constant), Entrepreneurial Orientation, Information Security Policy Enforcement, Information Security Policy Enforcement*Entrepreneurial Orientation

In table 4.58, Model 1 indicates that Information Security Policy Enforcement was statistically significant ($p < 0.10$; Beta value = 0.0543); Entrepreneurial Orientation was also statistically significant ($p < 0.10$). Equation 6 shows that for a 1-unit increase in Information Security Policy Enforcement, the Firm Performance is predicted to have a difference by 1.75, given that the Entrepreneurial Orientation is held constant. The regression coefficient associated with Entrepreneurial Orientation means that the difference in Firm Performance between SMEs with high entrepreneurial orientation and SMEs with low entrepreneurial orientation is .68, given that Information Security Policy Enforcement is held constant.

Firm Performance = 27.5 + 1.75Information Security Policy Enforcement + 0.68Entrepreneurial Orientation -- Equation (6)

Model 2 reveals the details of the inclusion of the interactive term in the model. Information Security Policy Enforcement was found to be significant (p=0.080 < 0.10, Beta value=0.7654). Entrepreneurial Orientation was found to be significant (p=0.0650 < 0.10, Beta value=1.2654), and Information Security Policy Enforcement*Entrepreneurial Orientation was also found to be significant (p=0.0540 < 0.10, Beta value=0.5652). On substitution of the coefficients in equation (5), we obtain:

Firm Performance = 24.3257 + 1.99(Information Security Policy Enforcement) + 1.4756(Entrepreneurial Orientation) + 0.3109(Information Security Policy Enforcement*Entrepreneurial Orientation) --- Equation (7)

Table 4.58 Moderated Multiple Regression Model Coefficients for Information Security Policy Enforcement

Model	**Coefficients**				
	B	**SE**	**Beta**	**t**	**p**
Constant	27.5	2.085		.2315	.0865
EO	.68	.0765	.4235	1.213	.0743
ISPE	1.75	.2543	.0543	1.185	.0782
Constant	24.3257	1.4962		61.9003	.0000
EO	1.4756	.1409	1.2654	1.9224	.0650
ISPE	1.99	.1783	.7654	1.4551	.0800
EO*ISPE	.3109	.0077	.5652	1.9237	.0540

The result for Table 4.58 indicates that for a 1-point increase in the Information Security Policy Enforcement, the Firm Performance is predicted to have a difference by 1.99, given that Entrepreneurial Orientation is held constant. The interpretation of the regression coefficients for the interaction term in Equation (7) is that there was a 0.3109 difference between the slope of Firm Performance on Information Security Policy Enforcement between SMEs with low entrepreneurial orientation and those with high entrepreneurial orientation. The slope regressing Firm Performance on Information Security Policy Enforcement is steeper for SMEs with high entrepreneurial orientation as compared to SMEs with low entrepreneurial orientation, as shown in figure 4.29. Results based on equation (7) led to the conclusion that there was a significant moderating effect of entrepreneurial orientation.

One progressively important model for protecting a firm's IT systems, and for decreasing rate of security breaches, is the formulation and application of a formal information security policy (Hinde, 2002). This shows that if an entrepreneurial orientation stance is embraced by all employees of top 100 medium-sized firms to enforce information security policy, then this would go a long way in ensuring adequate protection for a firm's IT systems, in turn translating to superior firm performance. In such a situation it is incumbent upon owner/managers to create a work environment that is conducive for maintaining an incessant state of proactiveness, innovativeness, and risk taking (Poon, Ainuddin & Junit, 2006). For instance, owner/managers establishing creativity training programmes that encourage employees to embrace an entrepreneurial orientation stance.

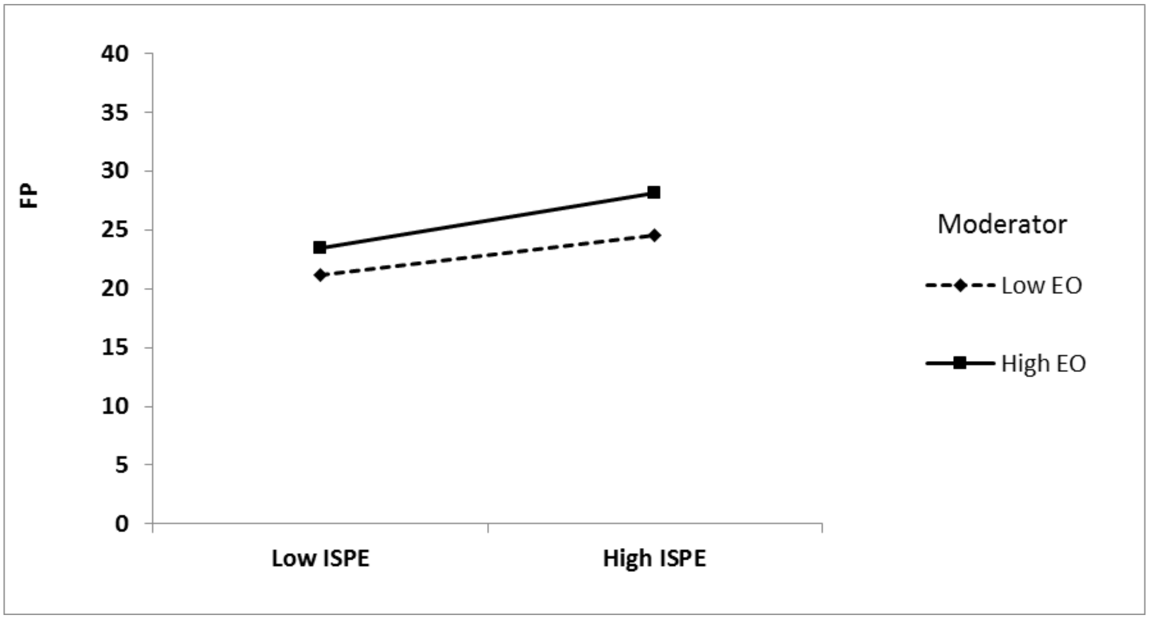


Figure 4.29 Slope of Firm Performance on Information Security Policy Enforcement for Entrepreneurial Orientation

4.12.2 Moderating Effect of Entrepreneurial Orientation on the Relationship Between Human-related Information Security Issues and Firm Performance

Table 4.59 shows that for Model 1, R = .615, R^2 = .379 and [F (2, 79) = 124.074, p = .0001]. The value of R^2 indicates that 37.9% of the variance in the Firm Performance is explained by Human-related Information Security Issues scores and Entrepreneurial Orientation. Model 2 shows the results after the interaction term (Human-related Information Security Issues*Entrepreneurial Orientation) was included in the equation. Table 4.59 also indicates that the inclusion of the interaction term resulted into an R^2 change of .0253, [F (1, 78) = 6.576, $p < 0.10$]. The results show a presence of significant moderating effect. To put it differently, the moderating effect of Entrepreneurial Orientation explains 2.53% variance in the Firm Performance, above and beyond the variance by Human-related Information Security Issues and Entrepreneurial Orientation. Thus the null hypothesis was rejected and therefore Entrepreneurial Orientation moderates the relationship between Human-related Information Security Issues and Entrepreneurial Orientation.

Table 4.59 Moderated Multiple Regression Model Summary for Human-related Information Security Issues

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.615[a]	.379	.363	.79815796	.379	124.074	2	79	.000
2	.623[b]	.382	.324	.76176051	.0253	6.576	1	78	.061

a. Predictors: (Constant), Entrepreneurial Orientation, Human-related Information Security Issues
b. Predictors: (Constant), Entrepreneurial Orientation, Human-related Information Security Issues, Human-related Information Security Issues*Entrepreneurial Orientation

In table 4.60, Model 1 indicates that Human-related Information Security Issues was statistically significant ($p < 0.10$; Beta value = 0.0731); Entrepreneurial Orientation was also statistically significant ($p < 0.10$). Equation 8 shows that for a 1-unit increase in Human-related Information Security Issues, the Firm Performance is predicted to have a difference by 1.0554, given that the Entrepreneurial Orientation is held constant. The regression coefficient associated with Entrepreneurial Orientation means that the difference in Firm Performance between SMEs with high entrepreneurial orientation and SMEs with low entrepreneurial orientation is 0.5895, given that Human-related Information Security Issues is held constant.

Firm Performance = 34.2316 + 1.0554Human-related Information Security Issues + 0.5895Entrepreneurial Orientation --- Equation (8)

Model 2 reveals the details of the inclusion of the interactive term in the model Human-related Information Security Issues was found to be significant (p=.0900 < 0.10, Beta value=0.4531). Entrepreneurial Orientation was found to be significant (p=0.0750 < 0.10, Beta value=1.1436), and Human-related Information Security Issues*Entrepreneurial Orientation was also found to be significant (p=0.0850 < 0.10, Beta value=0.3753). On substitution of the coefficients in equation (5), we obtain:

Firm Performance = 32.5 + 2.526 (Human-related Information Security Issues) + 0.8239 (Entrepreneurial Orientation) + 0.298 (Human-related Information Security Issues*Entrepreneurial Orientation) -- Equation (9)

Table 4.60 Moderated Multiple Regression Model Coefficients for Human-related Information Security Issues

Model	Coefficients				
	B	SE	Beta	t	p
Constant	34.2316	3.0765		.4371	.0000
EO	.5895	.0765	.2654	.1.3030	.0465
HRI	1.0554	.1871	.0731	.1.4570	.0294
Constant	32.5	1.5373		60.2003	.0000
EO	.8239	.5152	1.1436	1.8650	.0750
HRI	2.526	.4903	.4531	2.066	.0900
EO*HRI	.2980	.0037	.3753	1.0921	.0850

The result for Table 4.60 indicates that for a 1-point increase in the Human-related Information Security Issues, the Firm Performance is predicted to have a difference by 2.526, given that Entrepreneurial Orientation is held constant. The interpretation of the regression coefficients for the interaction term in Equation (9) is that there was a 0.298 difference between the slope of Firm Performance on Human-related Information Security Issues between SMEs with low entrepreneurial orientation and those with high entrepreneurial orientation.

The slope regressing Firm Performance on Human-related Information Security Issues is steeper for SMEs with high entrepreneurial orientation as compared to SMEs with low entrepreneurial orientation, as shown in figure 4.30. Results based on equation (9) led to the conclusion that there was a significant moderating effect of entrepreneurial orientation.

Information security culture is an approved method in which employees’ duties are carried out in the organization, and hence information security culture has a great impact on the aspect of improving performance, information policy and managerial effectiveness (Babatunde & Selamat, 2012). Training and awareness programmes on the other hand, enable employees to change their behavior from being security vulnerable to a more defensive element against security breaches (Kazemi et al., 2012).

The fact that entrepreneurial orientation enhances the relationship between human-related information security issues and firm performance is very vital to the owner/managers of top 100 medium-sized firms. Accordingly, these firms should strive to be risk-oriented, proactive and innovative, because these key dimensions put together exemplify an entrepreneurial orientation strategy which reflects a firm’s propensity to engage in entrepreneurial behavior in order to achieve its strategic objectives (Wiklund and Shephard, 2003; Rauch et al., 2009), and consequently enabling superior performance.

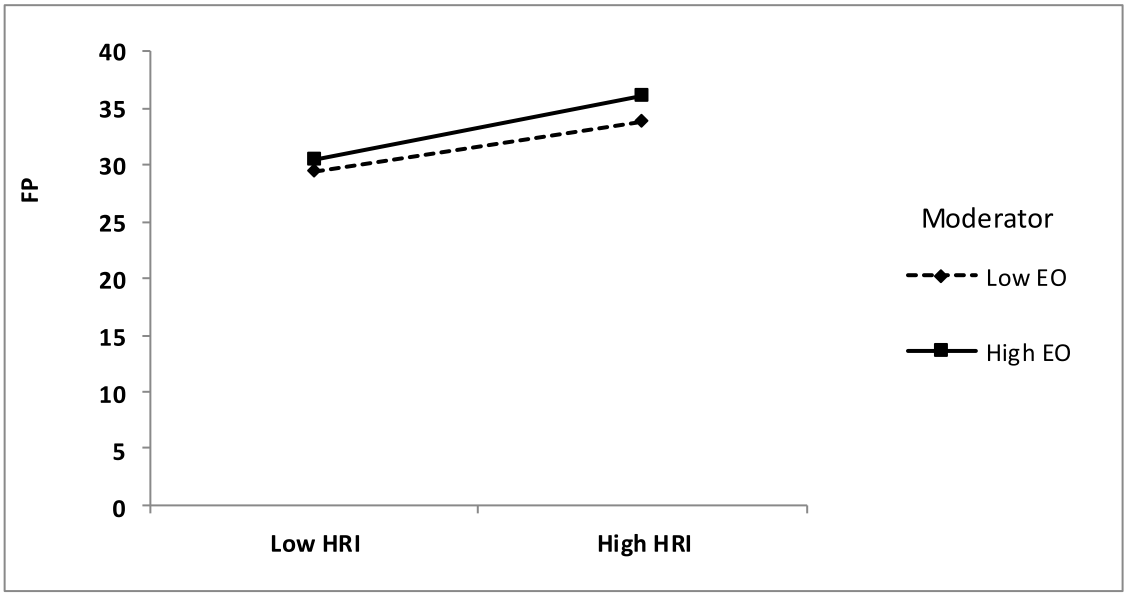


Figure 4.30 Slope of Firm Performance on Human-related Information Security Issues for Entrepreneurial Orientation

4.13 Summary of Hypothesis Testing Results

The results of hypothesis testing show that out of the six hypothesized relationships, only two were not significant. These were the relationship between information security policy enforcement and firm performance and the one between information technology competence and firm performance, meaning that the two independent variables did not contribute immensely to firm performance. But when the hypothesized relationship was tested at second order factor model level, the synergies brought out very good results. The hypothesized relationship between Non-technical factor and firm performance and that of Technical factor and firm performance were statistically significant at 5% α-level. This is an indication that second order model level provided more acceptable results than in the initial hypothesized relationships.

Table 4.61 Hypotheses Testing Results

Hypotheses	Sample Mean (M)	Standard Deviation (STDEV)	Standard Error (STERR)	T Statistics (|O/STERR|)	Initial Model Results	2nd Order Model Results	Conclusion
H_{01}: There is no relationship between top management commitment and firm performance in Kenya.	0.2251	0.1492	0.1492	1.5001	Significant at 10% α level	Significant at 5% α level	Reject H_{01}
H_{02}: There is no relationship between information security policy and firm performance in Kenya.	0.1725	0.1239	0.1239	1.2915	Significant at 10% α level		Reject H_{02}
H_{03}: There is no relationship between human-related information security issues and firm performance in Kenya.	0.0348	0.1428	0.1428	0.2411	Not Significant		Reject H_{03}
H_{04}: There is no relationship between information technology competence and firm performance in Kenya.	0.1567	0.1379	0.1379	1.0995	Not Significant	Significant at 5% α level	Reject H_{04}
H_{05}: There is no relationship between information security risk assessment and firm performance in Kenya.	0.247	0.0872	0.0872	3.224	Significant at 5% α level		Reject H_{05}
H_{06}: Entrepreneurial orientation does not moderate the relationship between information security management and firm performance in Kenya.	0.162	0.1209	0.1209	1.343	Significant at 10% α level		Reject H_{06}

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The summary of the study are presented in this chapter as guided by the specific objectives. These are followed by conclusions and recommendations. The chapter finally gives direction on areas of further research.

5.2 Summary of Findings

The general objective of this study was to investigate the moderating role of entrepreneurial orientation on the relationship between information security management and firm performance in Kenya. The study relied on theoretical and empirical studies on information security management and consequently developed a conceptual model of the relationship between the predictors and the dependent variable. The hypothesized relationships were then tested empirically.

Prior to the empirical test, certain assumptions about the variables used in the analysis were tested for, since most statistical tests rely upon them. The study also found no violation of the assumptions of normality, heteroscedasticity, multicollinearity, linearity, outliers, non-response bias and common method variance.

5.2.1 To Investigate the Influence of Top Management Commitment on Firm Performance in Kenya.

Top management commitment had a positive relationship with performance of medium-sized firms. Consequently, the null hypothesis was rejected. Top management commitment also had a statistically significant influence on the performance of medium-sized firms in Kenya. As well, top management commitment explained above average variation in firm performance. Out of the three factors of top management commitment, management participation and user satisfaction were found to have contributed significantly to top management commitment influencing performance of top 100 medium-sized firms in Kenya.

These results are consistent with the findings from other studies that have emphasized the significant role of top management commitment in effective information security management implementation. Kazemi, Khajouei and Nasrabadi (2012) identified top management commitment as the most important factor in effective information security management implementation, and that without it, none of the organizational plans will be implemented. Indeed, the priority given to information security appears to relate more to the attitude of senior management than the sector the business belongs to (ENISA, 2007).

5.2.2 To Establish the Influence of Information Security Policy Enforcement on Firm Performance in Kenya.

Information security policy enforcement had a relationship with performance of medium-sized firms. This necessitated rejection of the hypothesis that there is no relationship between information security policy enforcement and performance of medium-sized firms in Kenya. Two factors namely, right implementation and teamwork contributed to information security policy enforcement influencing performance of top 100 medium-sized firms in Kenya. However, information security policy enforcement had no statistically significant influence on firm performance.

This corroborates an empirical study by Doherty & Fulford (2005) on Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis, which suggested there was no statistically significant relationship between the adoption of information security policies and the incidents or severity of security breaches, and hence firm performance. These results contradict what has been discussed earlier about the benefits of security policies in organizations.

5.2.3 To Explore the Effect of Human-Related Information Security Issues (Culture, Awareness and Training) on Firm Performance in Kenya.

Human-related information security issues (culture, awareness and training) had a relationship with performance of top 100 medium-sized firms in Kenya. Consequently, the hypothesis that there is no relationship between human-related information security issues and performance of medium-sized firms in Kenya was rejected. As well, human-related information security issues had a statistically significant effect on firm performance in Kenya. Human-related information security issues also explained a substantial variation in firm performance. All the three factors of human-related information security issues, namely culture, awareness and training contributed significantly to the human-related information security issues influencing firm performance in Kenya.

These results are similar to findings of Kazemi, Khajouei and Nasrabadi (2012) who identified awareness and training programs as playing an important role in increasing employee awareness. The study emphasized that staff must be trained correctly, otherwise they will not function properly. Alnatheer and Nelson (2009) also identified security awareness and training as success factors for the implementation of information security management, in their study on A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. Ruighaver, Maynard and Chang (2007) in their study on Organizational Security Culture: Extending the End-User Perspective, identified culture as the single most important factor accounting for success or failure in an organization.

5.2.4 To Assess the Influence of Information Technology Competence on Firm Performance in Kenya.

Information technology competence had a relationship with performance of medium-sized firms. Two factors, namely knowledge of IS and experience of IS contributed to the information technology competence influencing performance of medium-sized firms in Kenya. Thus the hypothesis that there is no relationship between information technology competence and firm performance in Kenya was rejected. However, information technology competence did not have a statistically significant relationship with firm performance in Kenya.

Makadok (2001), in his study on Toward a Synthesis of the resource-based and dynamic-capability views of rent creations, found no statistically significant relationship between information technology competence and firm performance. Ray, Muhanna and Barney (2005) in their study on Information Technology and the Performance of the Customer Service Process: A resource-based Analysis, also found that there were no direct effects of three different information technology resources, that is, technical skills of information technology unit, managers' technology knowledge, and information technology spending, on the performance of the customer service process, leading to overall firm performance.

5.2.5 To Determine the Effect of Information Security Risk Assessment on Firm Performance in Kenya.

Information security risk assessment had a relationship with performance of medium-sized firms and all the three factors of information security risk assessment, namely threats and vulnerabilities, potential impact and likelihood of occurrence contributed significantly to the effect of information security risk assessment on performance of medium-sized firms in Kenya. Thus the hypothesis that there is no relationship between information security risk assessment and firm performance in Kenya was rejected.

This is in line with the findings of Gerber and von Solms (2005). In their study on Management of Risk in the Information Age, they identified information security risk assessment as one of the success factors in information security management leading to firm performance.

5.2.6 To Determine Whether Entrepreneurial Orientation Moderates the Relationship between Information Security Management and Firm Performance in Kenya.

To determine the moderating effect of entrepreneurial orientation on the relationship between information security management and performance of medium-sized firms in Kenya, hierarchical multiple regression was used to test for the significance of introducing the interaction between the predictors (information security management factor*entrepreneurial orientation) in each of the hypothesized relationship. Significant moderating effect was reported in the relationship between information security policy enforcement and performance of top 100 medium-sized firms in Kenya when the interaction term (information security policy enforcement*entrepreneurial orientation) was included. Similarly, significant moderating effect was reported in the relationship between human-related information security issues and performance of top 100 medium-sized firms in Kenya when the interaction term (human-related information security issues*entrepreneurial orientation) was included.

These results were corroborated when structural equation modeling (SEM) with moderation was carried out, where the interactions information security policy enforcement*entrepreneurial orientation, and human-related information security issues*entrepreneurial orientation were both found to be significant at 10% α level. Structural equation modeling with moderation was also carried out at second order level in order to test the significance for the synergies of the factors at a higher level. Prior to moderation, both technical (ITC and ISRA) and non-technical (TMC, ISPE and HRI) factors were found to be positively related to performance of top 100 medium-sized firms in Kenya and were statistically significant at 5% α level. This second order model result was found to be more satisfactory than the initial model where only top management commitment and information security risk assessment were found to be statistically significant.

When structural equation modeling with moderation was carried out, an insightful finding was noted. Moderated individually, that is, information technology competence*entrepreneurial orientation, and information security risk assessment*entrepreneurial orientation these factors did not result into significant interactions. But when synergized, that is, technical factor*entrepreneurial orientation produced significant interaction at 10% α level. This was a demonstration that synergy of factors produces improved interactions. It also demonstrated technological entrepreneurship suggesting that medium-sized firms should continue investing in technology for better performance. However, non-technical factor*entrepreneurial orientation interaction was not significant at 10% α level.

In summary, only the top management commitment factor did not show the presence of moderating effect even at higher order constructs probably because in all organizations, irrespective of the sector they are in, require the same level of commitment for their senior officers for effective performance.

5.3 Conclusions

Emanating from the analyses, top management commitment was found to have a statistically significant influence on performance of top 100 medium-sized firms in Kenya. This is in line with the neo-institutional theory framework which shows that senior management belief in information system security also influences senior management participation in information system security. The dynamic changes in technology call for huge investments in information security management. Therefore, the management are in a position not only to identify business niches and opportunities but also to make sufficient resources available for the implementation of information security management in the organization.

Essentially, top management commitment will accelerate the implementation of information security management initiatives as well as align information security management with the corporate objective and strategies, leading to overall better performance of the firm. It is also consistent with existing literature. Sharma and Yetton (2006) in their study on The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation, identified top management commitment as a success factor for managing information security. Liang, Saraf, Hu and Xue (2007) too, in their study on Assimilation of Enterprise Systems: The effect of Institutional Pressure and Mediating Role of Top Management. In any case, Covin and Slevin (1989) stated that entrepreneurial orientation is typically tested through top management, and so in small and medium-sized firms the owner-manager leading the firm greatly influences its culture and entrepreneurial manner. Thus it can be said that top management commitment can be used as a significant tool for better performance of medium-sized firms.

Human-related information security issues (culture, training and awareness) were also found to have a statistically significant influence on performance of top 100 medium-sized firms in Kenya. This is in line with the diffusion of innovations theory which centers on the conditions which increase or decrease the likelihood that a new idea, product, or practice will be adopted by members of a given culture. The same study emphasizes that mechanisms should be sought to encourage and foster an innovative culture in organizations since these are likely to facilitate the introduction, adoption and diffusion of innovations which, in turn, is likely to result in achievement of superior performance of medium-sized firms.

It is also in line with Deterrence Theory's shaming which is a technique for encouraging employees to adhere more to information security policies and training. In this study, this theory shows the importance of information security training in maximizing information systems security leading to overall firm performance. Anticipated shaming is also important as a method of encouraging employees to adhere to information security policies and training. Harris (2012) in his study on **S**haming as a Technique for Information Security Policy and Training Adherence identified information security training as one of the factors which is encouraged by Deterrence Theory's shaming technique. Human-related information security issues can therefore be used as a significant tool to ameliorate performance of medium-sized firms.

Schultz (2004) in his study on Security Training and Awareness - Fitting a Square Peg in a Round Hole, identified information security awareness as an important part of information security management and stated that increasing awareness of security issues is the most cost-effective control that a firm can implement. Hinde (2002) in his study on Security Survey Spring Crop suggested that the absence of awareness programs indicate a critical gap in effective security implementation, while Alnatheer and Nelson (2009) summed up and stated that security training and awareness programs are a fundamental component of effective information security strategy, leading to better firm performance. The top 100 medium-sized firms should adopt innovative teaching/learning methods because the current knowledge revolution requires innovative educational methods in the training of professionals. This places the learner at the center of the learning process and could have a positive impact on information security, leading to better performance of the medium-sized firms in Kenya.

Information Security Risk Assessment also had a statistically significant influence on performance of top 100 medium-sized firms in Kenya. Hong, Chi, Chao and Tang (2003) in their study on An Integrated System Theory of Information Security Management, identified Information Security Risk Assessment as one of the success factors of information security management. In line with this, risk management theory suggests that through organizational risk analysis and evaluation, the threats and vulnerabilities regarding information security could be estimated and assessed, and the evaluation results used for planning information security requirements and risk control measures, with the ultimate goal of reducing or minimizing information security risk to an acceptable level in an organization.

In this regard, through information security risk assessment, a medium-sized firm could take appropriate measures to protect information cost-effectively, in turn leading to better performance. In light of this it can be concluded that information security risk assessment is a cornerstone of information security management implementation that could lead to superior performance of the top 100 medium-sized firms.

Entrepreneurial Orientation was found to moderate two hypothesized relationships, that is, the relationship between information security policy enforcement and firm performance, and the relationship between human-related information security issues and firm performance. Also at second order structural equation modeling with moderation, the synergy between the technical factors, that is, information technology competence and information security risk assessment produced significant interaction. This was insightful considering that this study is advancing technological entrepreneurship. The top 100 medium-sized firms advancing technology entrepreneurship should adopt entrepreneurial orientation philosophy for superior performance. Undoubtedly, the interplay of information technology competence and information security risk assessment as moderated by entrepreneurial orientation could be said to be the face of technological entrepreneurship.

Technology entrepreneurship is an investment in a project that assembles and deploys specialized individuals and heterogeneous assets to create and capture value for the firm (Bailetti, 2012). This was also exemplified by the initial empirical results, where factors associated with high levels of the organization (top management), factors associated with technology (information security risk assessment) and factors associated with human capital (human-related information security issues) were significant, bringing together the decision makers, who must approve the information security budget, the technology itself, and the staff who must undergo the information security training and awareness process that would consequently inculcate the information security culture in the medium-sized firms.

The core finding of this study is that information security management factors had a positive and significant effect on the performance of top 100 medium-sized firms in Kenya. Similar findings were reported by Bose, Luo and Liu (2013) in their study on The Relationship between Information Security Investment and Organizational Performance: A Critical Review. Also, Hall, Sarkani and Mazzuchi (2011) in their study on Impacts of Organizational Capabilities in Information Security, confirmed significant and positive association between information security strategy implementation success and organization performance.

Additionally, Santhanam and Hartono (2003) in their study on Issues in Linking Information Technology Capability to Firm Performance also reported the same findings. This is in line with the theory of creative destruction (Schumpeter 1942) which proposes that companies holding monopolies based on incumbent technologies have less incentive to innovate than potential rivals, and therefore they eventually lose their technological leadership role when new radical technological innovations are adopted by new firms which are ready to take the risks. Indeed, the notion of ‘creative destruction’ comes as a result of a technological change, where certain rents become available to entrepreneurs.

These rents, also referred to as Schumpeterian rents which stem from risky initiatives and entrepreneurial insights in uncertain and complex environments, and later diminishing to innovations which cause market dislocations, are adopted. Foster and Kaplan (2001) emphasize that when the radical innovations eventually become the new technological paradigm, the newcomer companies leapfrog ahead of former leading firms. This is true with top 100 survey where you find almost half of the medium-sized firms missing in the subsequent ranking. Lastly, information security management is a structured process for continuous management of information security of an enterprise, and should be considered a long-term strategy of the organization (Badamas, 2008).

On the other hand, Garg, Curtis and Halper (2003) in their study on The Financial Impact of IT Security Breaches: What do Investors Think?, estimated that security incidents cost breached companies 0.5 to 1 percent of annual sales on average. Likewise, Cavusoglu Mishra and Raghunathan (2004) in their study on The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, found that the security breach announcements affected the value of breached firms. In short, these studies demonstrated negative performance of firms affected by security breaches.

Additionally, Ko and Dorantes (2006) in their study on The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation found out that security breach incidents resulted in decreased performance of the affected firms in the long-term. In contrast, however, Hovav and D’arcy (2003), based on data from 1998-2002, did not find evidence of a significant market response to breaches associated with denial-of-service (DOS) attacks. Similarly, Kannan, Rees and Sridhar (2007) found a negative, but statistically insignificant stock market response to denial-of-service (DOS) attacks. This amounts to strategic entrepreneurship at play.

Results of this study also indicated that entrepreneurial orientation significantly moderated the relationship between information security management and firm performance. Thus the results provide some exploratory information that hoped to deepen the understanding of the interrelationship between technology entrepreneurship, entrepreneurial orientation and firm performance. The World Economic Forum holds that the management of technology, innovation and information have emerged as key requirements for success in the 21st century (Claros, Altinger, Blanke, Drzeniek & Mia, 2006).

Therefore, companies, particularly medium-sized businesses in Kenya need to become more entrepreneurial in order to increase their competitiveness (Antoncic & Hisrich, 2001; Drucker, 2002) and survive and prosper in turbulent environments (Lumpkin & Dess, 1996). Being more entrepreneurial means increased entrepreneurial intensity levels (Morris, 1998), a trait that must have been exhibited by the firms that appeared in the 2013 Top 100 Survey.

Overall, the study has demonstrated positive relationship between technological entrepreneurship and performance of medium-sized firms in Kenya. It has also demonstrated that entrepreneurial orientation enhances the technological entrepreneurship and medium-sized firm performance relationship, meaning that a continued increase of entrepreneurial intensity levels will ensure that the relationship will continuously be positive. Certainly this is a model that can be adopted by medium-sized companies in Kenya as a way of enhancing their firm performance and thus allowing them to internationalize.

It is hoped that this study can provide insights for future research in this area and help medium-sized firms in Kenya and in the rest of the world to foster and implement effective information security management and entrepreneurial orientation as both are found to be the leading factors in enhancing firm performance. This study also fills the gaps identified at the literature review stage where it was revealed that limited attention has been paid to the moderating role of entrepreneurial orientation on the relationship between information security management and firm performance. Moreover, the few studies that have been done in the area of information security management mostly in Europe, Asia and the United States of America fail to relate information security management to firm performance. This study therefore has added value to existing literature by providing empirical information security management measures that medium-sized firms in Kenya can adopt in order to improve on their performance.

5.4 Recommendations

In general, the results provide practitioners with important insights by highlighting the benefits that medium-sized firms can derive through an effective implementation of information security management. In particular, small and medium enterprises with little or no information security management experience can gain a deeper understanding of this process to better protect their information assets. This is because the proposed model can serve as a guide for developing and implementing an information security management system within an organization.

Specifically, factors associated with technology need to be accorded special attention as they have shown to have the greatest impact on performance of top 100 medium-sized firms. Thus adoption of strategic orientation initiatives like password-based protection, use of biometrics and cryptography should be vigorously pursued by owners/managers of medium-sized firms. Investing in technology will enable these firms manage cybercrime, now ranking as one of the top four economic crimes in Kenya and globally, and the resulting losses that they undergo. Particularly, information security risk assessment has to be given first priority and resources availed if the top 100 medium-sized firms have to post better performance. This study therefore recommends that firms need to invest in information security management since it also ensures firm performance.

Top Management Commitment should be accorded priority number two as the commitment of the top managers (decision makers) and participation in information security initiatives gives an impression of their support. Undoubtedly, failure of the top management to support or understand the need for information security would result in an ineffective information security implementation, or worse still, in total failure. Another area requiring special attention in terms of investment is human-related information security issues consisting of culture, training and awareness. Proper training and awareness would inculcate an information security alertness culture in the employees, consequently improving performance of an organization. Top 100 medium-sized firms should therefore invest in the three major areas for better firm performance. Top management should also ensure there is an entrepreneurial culture within the firm.

Development of an information security policy will curb information insecurity which is a big obstacle to those entrepreneurial medium-sized firms wishing to internationalize. A policy on information sharing should also be included in the overall information security policy of firm, as a way of enhancing open innovation. Indeed the Kenyan government, as it tries to achieve Vision 2030, can develop an information security policy which will guide SMEs in adopting information security philosophy, considered to be a best practice for entrepreneurial firms.

Lastly, because the findings showed that entrepreneurial orientation moderates the relationship between information security management and firm performance, ways to cultivate or inspire entrepreneurial orientation behaviors and promote the context that supports such behaviors need to be formulated. This is because only when employees are able and willing to take proactive action, be innovative, and assume risks will the top 100 medium-sized firms realize sustainable competitive advantage and superior performance.

In summary, factors associated with technology need to be enhanced by including them in the mission and vision statements of firms and making them part of their code of conduct as the study has demonstrated positive relationship between technological entrepreneurship and performance of medium-sized firms. Entrepreneurial orientation concept on the other hand, should be a management philosophy in majority of top 100 medium-sized firms. Finally, top 100 medium-sized firms should be encouraged to increase their entrepreneurial intensity levels for superior performance.

5.5 Areas of Further Research

The study of information security management concentrated on only five sub-variables. It was not possible to study all factors that determine success of information security management. Without a doubt, other factors come into the interplay and provide perceptive results to the issue of information security management influencing the performance of medium-sized firms in Kenya. The moderating variable, on the other hand, concentrated on only three determinants of entrepreneurial orientation. Future research should concentrate on all the five determinants.

Secondly, the study relied on cross-sectional data survey where the respondents were asked to assess viewpoints on the item in the instrument. But some success factors of information security management are known to be strategic and dynamic in nature. Therefore, a longitudinal study would be more preferable as it could provide a better perspective of the effect of information security management on the firm performance in Kenya in addition to further informing the policy frameworks of information security management.

Lastly, the findings presented in this study are based on evidence gathered from medium-sized firms that participated in the 2013 Top 100 Survey. Future research should be extended to financial institutions whose allure to cyber criminals are the millions of financial transactions carried out every day.

REFERENCES

Aas, K. & Haff, I. H. (2006). The Generalised Hyperbolic Skew Student's *t*-distribution. *Journal of Financial Econometrics, 4*, 275-309.

Abbott, M. L., & McKinney, J. (2013). *Understanding and applying research design*. (1st ed.). Somerset, NJ: John Wiley & Sons.

Abdi, H., & Williams, L. J. (2010). Principal component analysis. *Wiley Interdisciplinary Reviews: Computational Statistics, 2*(4), 433-459.

Abu-Musa, A. A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security, 18*(4), 226-276.

Aguinis, H., & Gottfredson, R. K. (2010). Best practice recommendations for estimating interaction effects using moderated multiple regression. *Journal of organizational behavior, 31*(6), 776-786.

Al-Awadi, M., A. (2009). *A study of Employees' Attitudes Towards Organisational Information Security Policies in the UK and Oman*. (Published Doctoral dissertation, University of Glasgow). Retrieved from http://theses.gla.ac.uk/860/.

Al-Awadi, M. & Renaud, K. (2008, 06 17). *Success factors in information security implementations in organizations.* Retrieved 04 17, 2013, from dcs: http://www.dcs.gla.ac.uk/~karen/Papers/sucessFactors2.pdf

Alfawaz, S. M. (2011). *Information security management: A case study of an information security culture*. (Queensland University of Technology). Retrieved from: http://eprints.qut.edu.au/view/types/qut=5Fthesis/2011.html

Alnatheer, M., & Nelson, K. J. (2009). *A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.* In: 7th Australian Information Security Management Conference, 1-3 December 2009, Kings Perth Hotel, Perth.

Alshawaf, A. H., Ali, J. M. H. & Hasan, M. H. (2005). A benchmarking framework for information systems management issues in Kuwait. *Benchmarking: An International Journal, 12*(1), 30-44.

Analoui, F., & Samour, A. (2012). The managers' characteristics and their strategy development in the Palestinian NGOs: An empirical study in Palestine. *Journal of Management Development, 31*(7), 691-699.

Anastas, J. W. (1999). *Research Design for Social Work and the Human Services*. (2nd ed.). New York: Columbia University Press.

Anderson, J. C. & Gerbing, D. W. (1988). Structural equation modeling in practice: a review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Antoncic, B., & Hisrich, R. D. (2001). Intrapreneurship: Construct refinement and cross-cultural validation. *Journal of Business Venturing 16*(5), 495–527.

Antoncic, B., & Hisrich, R. D. (2003). Clarifying the intrapreneurship concept..Emerging Issues in Corporate Entrepreneurship. *Journal of Management, 29*(3), 671-694.

Arbuckle, J. L. & Wothke, W. (1999). *AMOS 4.0 User's Guide*. Chicago: Smallwaters

Argyrous, G. (2005). *Statistics for research: With a guide to SPSS*. London: Sage

Armstrong, J. S. & Overton, T. S. (1977). Estimating Nonresponse Bias in Mail Surveys. *Journal of Marketing Research, 14*(3), 396–402.

Ashrafi, R. & Murtaza, M. (2008). Use and impact of ICT on SMEs in Oman. *The EJISE, 11*(3), 125-138.

Autry, C. W., & Bobbitt, L. M. (2008). Supply Chain Security Orientation: Conceptual Development and a Proposed Framework. *The International Journal of Logistics Management, 19*(1), 42-64.

Avolio, B. J., Yammarino, F. J. & Bass, B. M. (1991). Identifying common method variance with data collected from a single source: an unresolved sticky issue. *Journal of Management, 17*(3), 571-87.

Babatunde, D. A., & Selamat, M. H. (2012). Investigating Information Security Management and Its Influencing Factors in the Nigerian Banking Industry: a Conceptual Model. *International Journal on Social Science & Art, 2*(2), 55-59.

Babbie, E. (1990). *Survey research methods*. Belmont, CA: Wadsworth Publishing.

Babbie, E. & Mouton, J. (2002). *The practice of social research*. Oxford: Oxford University Press.

Bacha, E. (2012). The impact of information systems on the performance of the core competence and supporting activities of a firm. *Journal of Management Development, 31*(8), 752-763.

Badamas, M. A. (2008). Exploring the relationship between Total Quality Management and Information Security Management. *Industrial Management & Data Systems, 107*(3), 451-474.

Baggili, I. (2009). *Effects of anonymity, pre-employment integrity and antisocial behavior on self-reported cyber-crime engagement: An exploratory study*. (Published Doctoral dissertation University of Purdue). Retrieved from: http://www.purdue.edu/

Bahl, S. & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. *Information Management & Computer Security, 22*(1), 2-23.

Bailetti, T. 2012. Technology Entrepreneurship: Overview, Definition, and Distinctive Aspects. *Technology Innovation Management Review, 5*, 5-12.

Bailey, K. D. (1987). *Methods of social research* (3rd ed.). New York: Free Press.

Bakari, J. K. (2007). *A holistic approach for managing ICT security in non-commercial organizations - A case study in a developing country*. (Published doctoral dissertation, Stockholm University). Retrieved from http://www.opendoar.org.

Barman, S. (2002). *Writing Information Security Policies*. Indianapolis, IN: New Riders Publishing.

Barney, J. B., & Arikan, A. M. (2001). *The resource-based view: Origins and implications*. Oxford: Blackwell.

Bassellier, G., Reich, B. H. & Benbasat, I. (2001). Information technology competence of business managers: a definition and research model. *Journal of Management Information Systems, 17*(4), 159-182.

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management, 24*(7), 991-1010.

Belsley, D. A., Kuh, E., & Welsch, R. E. (2004). *Regression Diagnostics: Identifying Influential Data and Sources of Collinearity*. Hoboken, NJ: John Wiley & Sons, Inc.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly, 24*(1), 169-196.

Bhattacharyya, D. K. (2011). *Human Resource Research Methods*. New Delhi: Oxford University Press.

Billing, T. K., Mukherjee, D., Kedia, B. L., & Lahiri, S. (2010). Top executives' international expertise commitment: exploring potential antecedents. *Leadership & Organization Development Journal, 31*(8), 687-704.

Bingham, C., Eisenhardt, K. M. & Furr, N. (2007). What makes a process a capability? Heuristics, strategy and effective capture of opportunities. *Strategic Entrepreneurship Journal, 1*, 27-47.

Bishop, D. I., & Hertenstein, M. J. (2004). A confirmatory factor analysis of the structure of temperament questionnaire. *Educational and Psychological Measurement, 64*(6), 1-11.

Bollen, K. A. (1989). *Structural Equations with Latent Variables*. Somerset, NJ: John Wiley & Sons.

Boonmak, S. (2008). Influence of Human Factors on Information Security Measures Effectiveness under Ethic Issues. *8th Global Conference on Business & Economics*, (pp. 1-55). Florence, Italy.

Bordens, K. S., & Abbott, B. B. (2014). *Research design and methods: A process approach* (9th ed.). San Francisco: McGraw Hill.

Bose, A. (2009, 09 24). *Measurement & Scaling*. Retrieved 06 21, 2013 from bimtech: http://210.212.115.113:81/Amarnath%20Bose/PrePhD/StudyMaterial/MeasurementAndScaling.pdf.

Bose, R., Luo, X., & Liu, Y. (2013). The Relationship between Information Security Investment and Organizational Performance: A Critical Review. *Proceedings of Annual Meeting of the Northeast Decision Sciences Institute* (pp. 305-319). New York: Wiley. Retrieved 08 03, 2013, from http://www.nedsi.org/proc/2013/proc/p121026006.pdf.

Bougaardt, G. & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *Electronic Journal Information Systems Evaluation, 14*(2), 167-178.

Bourke, P. (2011, 05 27). *Security breaches cost 47% of SMEs up to $20,000*. Retrieved 03 01, 2013, from Kochie's Business Builders: http://au.smallbusiness.yahoo.com/technology/.

Bowen, M., Morara, M., & Mureithi, S. (2009). Management of Business Challenges Among Small and Micro Enterprises In Nairobi-Kenya. *KCA Journal of Business Management*, 2(1), 16-31.

Box, G. E. P., & Jenkins, G. (1976). *Time Series Analysis: Forecasting and Control*. San Francisco: Holden-Day.

Braber, F., Hogganvik, I., Lund, S., Stolen, K. & Vrallsen, F. (2007). Model-based security analysis in seven steps - a guided tour to the CORAS method. *BT Technology Journal, 25*(1), 101-117.

Bret, W., Ted, B., & Andrys, O. (2010). Exploratory Factor Analysis: A Five Step Guide for Novices. *Journal of Emerging Primary Health Care, 8*(3), 101-124.

Brorstrom, B. (2002). The world's richest municipality: The importance of institutions for municipal development. *Journal of Economic Issues, 36*(4), 55-78.

Bryman, A. (2012). *Social research methods* (4th ed.). New York: Oxford University Press.

Bryman, A., & Bell, E. (2007). *Business research methods* (2nd ed.). New York: Oxford University Press.

Business Daily (BD). (2012, October 28). *SMEs play a crucial role in Kenyan economy*. Retrieved August 04, 2013, from BD: http://www.businessdailyafrica.com.

Byrne, B. M. (2001). *Structural Equation Modeling with AMOS, Basisc Concepts, Applications, and Programming*. Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9*(1), 69–104.

Cefis, E., & Ciccarelli, M. (2005). Profit differentials and innovation. *Economics of Innovation and New Technology, 14*(5), 43-61.

Chadwick, K., Barnett, T., & Dwyer, S. (2001). Entrepreneurial Orientation, Organizational Culture, and Firm Performance: An Empirical Study in the Banking Industry. *Journal of Applied Management and Entrepreneurship, 6* (3), 3-17.

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data, 107*(3), 438-458.

Chang, S.E., & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

Chen, F. F., Sousa, K. H., & West, S. G. (2005). Testing Measurement Invariance of Second-Order Factor Models. *Structural Equation Modeling, 12*(3), 471–492.

Chimi, C. J. & Russell, D. L. (2009). The Likert Scale: A Proposal for Improvement Using Quasi-Continuous Variables. *In The Proceedings of the Information Systems Education Conference*, Washington DC: 1542-7382.

Chun, H., Kim, J., Morck., R., & Yeung, B. (2007). Creative destruction and firm-specific performance heterogeneity. *Journal of Financial Economics, 18*(2), 64-128.

Claros, A. L., Altinger, L., Blanke, J., Drzeniek, M., & Mia, I. (2006). The global competitiveness index: Identifying the key elements of sustainable growth. *The Global Competitiveness Report 2006-2007. 1*, pp. 3-50. Geneva: The World Economic Forum. Retrieved 07 29, 2014.

Cohen, J., Cohen, P., West, S. G., Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences*. Lawrence Erlbaum Associates: London.

Collman, J. & Cooper, T. (2007). Breaching the security of the kaiser permanente internet patient portal: the organizational foundations of information security. *Journal of the American Medical Informatics Association, 14*(2), 239-243.

Cook, T. D., & Campbell, D. T. (1979). *Quasi-Experimentation: Design & Analysis Issues for Field Settings*. Boston: Houghton Muffin.

Cooper, D. R., & Schindler, P. S. (2003). *Business research methods*. (8th ed.). Boston: McGraw-Hill.

Cooper, D. R., & Schindler, P. S. (2011). *Business Research Methods*. (11th ed.). New York: McGraw-Hill.

Costello, A. B. & Osborne, J. (2005). Best practices in exploratory factor analysis: four recommendations for getting the most from your analysis. *Journal of practical assessment, research & evaluation, 10*(7), 173-178.

Covin, J. G. & Lumpkin, G. T. (2011). Entrepreneurial orientation theory and research: reflections on a needed construct. *Entrepreneurship Theory and Practice, 35*(5), 855-872.

Covin, J. G. & Slevin, D. P. (1989). Strategic Management of Small Firms in Hostile and Benign Environments. *Strategic Management Journal. 10*(1), 75-87.

Covin, J. G. & Slevin, D. P. (1991). A Conceptual Model of Entrepreneurship as Firm Behavior. *Entrepreneurship Theory and Practice, 16*(1), 7-25.

Covin, J. G., & Slevin, D. P. (2002). *The entrepreneurial imperatives of strategic leadership*. Oxford: Blackwell Publishers.

Cronbach, L. J. (1951). Coefficient alpha and the internal Structure of tests. *Psychometrika, 16*(3), 297-334. Retrieved 05 13, 2013, from http://psych.colorado.edu/.

Cronbach, L. J. (2004). My current thoughts on coefficient alpha and successor procedures. *Educational and Psychological Measurement 64*, 391-418.

Computer Security Institute (CSI). (2010, 08 29). *2010/2011 Computer Crime and Security Survey*. Retrieved 03 01, 2013, from gocsi: http://www.gocsi.com/.

Cresswell, J. W., & Clark, V. L. P. (2011). *Designing and conducting mixed methods research*. Los Angeles: Sage.

Cunningham, E. (2008). *Structural Equation Modeling using AMOS 6.0*. Melbourne: Swinburn University of Technology.

Damanpour, F., & Wischnevsky, J. D. (2006). Research on innovation in organizations: Distinguishing innovation-generating from innovation-adopting organizations. *Journal of Engineering and Technology Management, 23*(4), 269-291.

Dej, D. (2007). Motivation to become entrepreneur: In Leon, M., & Gorgievski, M. (Eds), *Psychology of entrepreneurship research and education* (pp. 57-64), printed in Spain.

Dess, G. G., & Picken, J. C. (1999). *Beyond productivity: How leading companies achieve superior performance by leveraging their human capital*. New York: AMACOM.

DeVellis, R. F. (2003). *Scale Development: Theory and Applications*. Thousand Oaks, CA: Sage Publications.

Dia, M. (1996). African Management in the 1990s and Beyond: Reconciling Indigenous and Transplant Institutions. Washington, DC: The World Bank.

DiMaggio, P. J. & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-159.

Dhillon, G. (1999). Managing and Controlling Computer Misuse. *Information Management & Computer Security, 7*(4), 171-175.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ: Wiley.

Diamond, A. M. (2006, 05 26). *Schumpeter's Creative Destruction: A Review of the Evidence*. Retrieved 07 12, 2013, from cba: http://cba.unomaha.edu/

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18* (2), 21-39.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. *15th European Conference on Information Systems* (pp. 1560-1571). St. Gallen, Switzerland.

Dong, X. (2009). The linkage between entrepreneurial intensity and firm performance: The evidence from China's SMEs. *International Conference on Industrial Mechatronics and Automation* (pp. 1-17). Chengdu: ICIMA 2009. Retrieved 11 27, 2013.

Doty, D. H., & Glick, W. H. (1998). Common methods bias: Does common methods variance really bias results? *Organizational Research Methods, 1*, 374-406.

Drost, E. A. (2011). Validity and Reliability in Social Science Research. *Education Research and Perspectives, 38*(1), 105-123.

Drucker, P. F. (1985). *Innovation and Entrepreneurship*. New York, NY: Harper and Row.

Drucker, P. F. (2002). *Innovation and entrepreneurship*. Oxford: Butterworth-Heineman.

Dutton, J. E., & Ashford, S. J. (1993). Selling issues to top management. *Academy of Management Review, 18*(3), 397-428.

Eloff, J. H. P. & Eloff, M. M. (2003). Information security management - a new paradigm. *ACM, 5*(1), 130-136.

European Network and Information Security Agency (ENISA) (2007). *Information Security Awareness Initiatives: Current Practice and the Measurement of Success*. Crete: ENISA.

European Commission. (2013, 02 05). *Small and medium-sized enterprises (SMEs).* Retrieved 02 23, 2013, from European Commission: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm

Farndale, E., Hope-Hailey, V., & Kelliher, C. (2010). High Commitment Performance Management: The Roles of Justice and Trust. *Personnel Review, 40*(1), 5-23.

Feigenbaum, A. & Thomas, H. (1988). Attitudes towards risk and the risk/return paradox. *Academy of Management Journal, 31*, 85-106.

Ferrier, W. J. & Lee, H. (2002). Strategic aggressiveness, variation, and surprise: How the sequential pattern of competitive rivalry influences stock market returns. *Journal of Managerial Issues, 14*(2), 162-180.

Field, A. (2009). *Discovering Statistics using SPSS.* Thousand Oaks, CA: Sage Publications.

Fischer, R. (2006). Congruence and functions of personal and cultural values: do my values reflect my culture’s values? *Personality and Social Psychology Bulletin, 32*(11), 1419-31.

Fisher, R. A. (1926). The arrangement of field experiments. *Journal of the Ministry of Agriculture of Great Britain, 33*, 503-513.

Flynn, M., Doodley, L. & Cormican, K. (2003). Idea management for organizational innovation. *International Journal of Innovation Management, 7*(4), 417-442.

Foster, R. N. & Kaplan, S. (2001). *Creative Destruction: Why Companies that are Built to Last Underperform the Market - and How to Successfully Transform Them*. (1st ed.). New York: Currency.

Fraser, S. W., Conner, M. & Yarrow, D. (2003). *Thriving in Unpredictable Times: A Reader on Agility in Health Care*. Chichester: Kingsham Press.

Frazier, P. A., Tix, A. P. & Barron, K. E. (2004). Testing moderator and mediator effects in counseling psychology research. *Journal of Counseling Psychology, 51*(2), 115-134.

Garg, A., Curtis, J. & Halper, H. (2003). The financial impact of IT security breaches: what do investors think? *Information Systems Security, 12*(1), 22-33.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security 24*, 16-30.

Ghotbi, A., & Gharechehdaghi, N. N. (2012). Evaluating the Security Actions of Information Security Management System in the Electronic Stock Commerce, and Providing the Improvement Strategies. *Journal of Basic and Applied Scientific Research, 2*(3)3046-3053.

Gibson, W. (1984). *Neuromancer*. London: Herper Collins.

Global Economic Crime Survey. (2011, 11 15). *A step ahead: Economic Crime in Kenya.* Retrieved 02 21, 2013, from pwc: http://www.pwc.com/.

Godfrey, P. C. & Hill, C. W. (1995). The problem of unobservables in strategic management research. *Strategic Management Journal, 16*, 519-533.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security, 19*(1), 33-56.

Graham, D. J. & Midgley, N. G. (2000). Graphical representation of particle shape using triangular diagrams: an Excel spreadsheet method. *Earth Surface Processes and Landforms, 25*(13), 1473-1477.

Gray, K. R. (2000). Small-scale manufacturing in Kenya: Characteristics, Problems and Sources of Finance. *Journal of Small Business Management, 29*(1), 23-37.

Greve, H. R. (2008). A behavioral theory of firm growth: sequential attention to size and performance goals. *Academy of Management Journal, 51*(3), 476-494.

Gupta, M. (2011). *Three essays on information technology security management in organizations*. (Published Doctoral dissertation, State University of New York at Buffalo). Retrieved from http://search.proquest.com/docview/854059025.

Gupta, P. K. (2011). Risk management in Indian companies: EWRM concerns and issues. *The Journal of Risk Finance, 12*(2), 121-139.

Hafiz, B., & Shaari, J. A. N. (2013). Confirmatory factor analysis (CFA) of first order factor measurement model-ICT empowerment in Nigeria. *International Journal of Business Management and Administration, 2*(5), 1-8.

Hair, J., Tatham, R. L., Anderson, R. E. & Black, W. (2006). *Multivariate Data Analysis*. (6th ed.). Upper Saddle River, NJ: Pearson Prentice-Hall.

Hair, J. F., Black, W. C., & Babin, B. J. (2010). *Multivariate Data Analysis: A Global Perspective*. Upper Saddle River, NJ: Pearson Prentice-Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-151.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155-176.

Hambrick, D. C. & Mason, P. A. (1984). Upper echelons: the organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193-206.

Harris, M. A. (2012). **S**haming as a technique for information security policy and training adherence. *Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA March 23rd-24th, 2012*. Shaming and IS Security Policy and Training. 92-97.

Heilbrunn, S. (2008). Factors influencing entrepreneurial intensity in communities. *Journal of Enterprising Communities: People and Places in the Global Economy, 2*(1), 37-51.

Hesterberg, T. (2003). *Bootstrap methods and permutation tests*. New York: W. H. Freeman and Company.

Hitt, M., Ireland, R., Camp, S. & Sexton, D. (2001). Guest editors' introduction to the special issue strategic entrepreneurship: entrepreneurial strategies for wealth creation. *Strategic Management Journal, 22*, 479-491.

Hinde, S. (2002). Security survey spring crop. *Computer & Security, 21*(4), 310-32.

Hodgetts, R. M., & Kuratko, D. F. (2001). *Effective small business management* (7th ed.). New York: Wiley.

Hone, K. & Eloff, J. (2002). What makes an effective information security policy? Network Security, 6(1), 14-16.

Hong, K., Chi, Y., Chao, L. R. & Tang, J. (2003). An integrated system theory of information security management. *Journal of information management & computer security, 11*(5), 243-248.

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

Hovav, A., & D'arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firm. *Risk Management and Insurance Review, 6*, 97-121.

Hoyt, R. E. & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *Journal of Risk and Insurance, 78*(4), 795-822.

Hu, L. T. & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. *Structural Equation Modeling, 6*(1), 1-55.

Hu, Q., Hart, P. J. & Cooke, D. (2007). The role of external and internal influences on information systems security: A neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153-172.

Huang, K., Wang, K. Y., Chen, K., & Yien, J. (2011). Revealing the Effects of Entrepreneurial Orientation on Firm Performance: A Conceptual Approach. *Journal of Applied Sciences, 11*(6), 3049-3052.

Huang, S., Lee, C., & Kao, A. (2006). Balancing performance measures for information security management. *Industrial Management & Data Systems, 106*(2), 242-255.

Hughes, M. & R. E. Morgan. (2007). Deconstructing the relationship between entrepreneurial orientation and business performance at the embryonic stage of firm growth. *Industrial Marketing Management, 36,* 651-661.

Hunton, J., Lippincott, B. & Reck, J. L. (2003). Enterprise resource planning systems: Comparing firm performance of adopters and nonadopters. *International Journal of Accounting Information Systems, 4*(3), 165-184.

Information Technology Governance Institute (ITGI) (2006). *Information Security Governance, Guidance for Boards of Directors and Executive Management* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.

Israel, G. D. (2012, 06 12). *Sampling: Determining sample size.* Retrieved 05 13, 2013, from University of Florida IFAS Extension: http://edis.ifas.ufl.edu/pd006.

Ireland, R., Hitt, M., Camp, S., & Sexton, D. (2001). Integrating entrepreneurship and strategic management actions to create firm wealth. *Academy of Management Executive, 15*(1), 49-63.

Ireland, R. D., Hitt, M. A., & Sirmon, D. G. (2003). A model of strategic entrepreneurship: the construct and its dimensions. *Journal of Management 29*(6), 963-989.

Ireland, R. D. & Hitt, M. A. (2005). Achieving and maintaining strategic competitiveness in the 21st century: The role of strategic leadership. *Academy of Management Executive, 19*(4), 65-77.

Ireland, R. D., Kuratko, D. F., & Morris, M. H. (2006). A Health Audit for Corporate Entrepreneurship: Innovation at all Levels - Part 2. *Journal of Business Strategy,* 27(2), 21-30.

Ireland, R. D., Covin, J. G. & Kuratko, D. F. (2009). Conceptualizing corporate entrepreneurship strategy. *Entrepreneurship: Theory & Practice, 33*(1), 19-46.

Jackson, D. L., Gillaspy, J. A., & Purc-Stephenson, R. (2009). Reporting practices in confirmatory factor analysis: An overview and some recommendations. *Psychological Methods*, *14*(1), 6-23.

Jap, S. D., & Anderson, E. (2004). Challenges and Advances in Marketing Strategy Field Research. Invited chapter in *Cool Tools for Assessing Marketing Strategy Performance*, eds. Christine Moorman and Don Lehmann, Marketing Science Institute, 269-292.

Johnson, A. M. (2005). The technology acceptance model and the decision to invest in information security. In *The 2005 southern association of information systems conference, 114-118*.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of mixed methods research*, *1*(2), 112-133.

Juma, V. (2011, October 06). Kenya: Services top list of fastest growing mid-sized firms. *BD*. Retrieved from http://allafrica.com/stories.

Kannan, A., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: an empirical analysis. *International Journal of Electronic Commerce, 12,* 69-91.

Kane, M. T. (2006). Validation. *Educational measurement, 4*(2), 17-64

Karimpanal, A. (2012, 04 17). The Cost of a Security Breach. Retrieved 03 01, 2013, from cnet: http://in.hp-makeitmatter.asia.cnet.com/the-cost-of-a-security-breach-10000105.htm.

Kassner, M. (2009, 06, 04). 10 ways to avoid IT security breaches. Retrieved 03 01, 2013, from techrepublic: http://www.techrepublic.com/blog/10-things/-10-ways-to-avoid-it-security-breaches/.

Kazemi, M., Khajouei, H. & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, *6*(14), 4982-4989.

Keel, R. (2005, 10 10). *Rational choice and deterrence theory*. Retrieved 02 28, 2013, from umsl: http://www.umsl.edu/~rkeel/200/ratchoc.html.

Ketchen, D. & Palmer, T. (1999). Strategic responses to poor organizational performance: a test of competing perspectives. *Journal of Management, 25*(5), 683-706.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126.

Kim, G., Kim, S., & French, A. M. (2014). What increases firms' performance of information security management and the role of regulatory pressure. *PACIS 2013 Proceedings.* Paper 100.

Kimwele, M., Mwangi, W., & Kimani, S. (2010). Adoption of Information Technology Security Policies: Case Study of Kenyan Small and Medum Entreprises (SMEs). *Journal of Theoretical and Applied Information Technology*, *18* (2), 1-11.

Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information Technology Security Management in Kenyan Small and Medium Enterprises. *International Journal of Computer Science and Information Technologies*, *2*(1), 517-525.

Kline, R. B. (2005). *Principles and Practice of Structural Equation Modeling* (2nd ed.). New York: The Guilford Press.

Kluge, J., Meffert, J., & Stein, L. (2000). The German road to innovation. *The McKinsey Quarterly*, *2*(5), 99-105.

Knapp, K. J. (2005). *A Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test*. (Published Doctoral dissertation, Auburn University). Retrieved from http: http://etd.auburn.edu/.

Knapp, K. J., Marshall, T. E., Rainer, E. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Kock, H., & Ellstrom, P. (2011). Formal and integrated strategies for competence development in SMEs. *Journal of European Industrial Training, 35*(1), 71-88.

Kombo, D. K., & Tromp, D. L. A. (2009). *Proposal and Thesis Writing: An Introduction*. Nairobi: Don Bosco Printing Press.

Koong, K. S., Merhi, M. I., & Sun, J. (2013). Push and pull effects of homeland information security incentives. *Information Management & Computer Security, 21*(3), 155-176.

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). New Delhi: New Age International.

Kothari, C. R. (2009). *Research Methodology: Methods and Techniques* (5th ed.). New Delhi: New Age International.

Koong, K. S., Merhi, M. I., & Sun, J. (2013). Push and pull effects of homeland information security incentives. *Information Management & Computer Security, 21*(3), 155-176.

Koul, R. B. (2008). Educational Research and Ensuring Quality Standards. *E-journal of All India Association for Educational Research (EJAIAER), 20*(3), 1-8.

Kroon, B., Voorde, K., & Timmers, J. (2013). High performance work practices in small firms: a resource-poverty and strategic decision-making perspective. *Small Business Economics, 41*(1), 71-91.

Kuratko, D. F., Hornsby, J. S., & Goldsby, M. G. (2007). The Relationship of Stakeholder Salience, Organizational Posture, and Entrepreneurial Intensity to Corporate Entrepreneurship. *Journal of Leadership & Organizational Studies, 13*(4), 56-72.

Kusumawardhani, A. (2013). *The Role of Entrepreneurial Orientation in Firm Performance: A Study of Indonesian SMEs in the Furniture Industry in Central Java*. (Published doctoral dissertation, Wollongong University). Retrieved from http://ro.uow.edu.au/theses/3895.

Kyobe, M. (2008, 02 11). *Evaluating Information Security within SMEs engaged in E-commerce in South Africa.* Retrieved 03 01, 2013, from isbe: http://www.isbe.org.uk/Kyobe.

Kyrgidou, L. P., & Hughes, M. (2010). Strategic entrepreneurship: origins, core elements and research directions. *European Business Review, 22*(1), 43-63.

Lacey, D., & James, B.E. (2010, 03 10). *Review of Availability of Advice on Security for Small/Medium Sized Organisations.* Retrieved 02 28, 2013, from ico.: http://www.ico.gov.uk/.

Lane, T. (2007). *Information security management in Australian Universities - An exploratory analysis.* (Published Doctoral dissertation, Queensland University of Technology). Retrieved from: http://eprints.qut.edu.au/16486/1/Tim_Lane_Thesis.pdf.

Latip, N. A. M., Salleh, M. I., Omar, B., & Yaakub, K. B. (2013). A Resource-based Perspective on Technological Competencies and Relationship Performance: An Empirical Analysis. *South East Asia Journal of Contemporary Business, Economics and Law, 3*(2), 18-22.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, (31)1, 59-87.

Liang, T., You, J., & Liu, C. (2010). A resource-based perspective on information technology and firm performance: a meta analysis. *Industrial Management & Data Systems, 110*(8), 1138-1158.

Liao, J., Murphy, P. J., & Welsch, H. P. (2005). Developing and validating a construct of entrepreneurial intensity. *New England Journal of Entrepreneurship 8*(2), 31-38.

Lichtenstein, S. (1996). Factors in the selection of a risk assessment method. *Information Management & Computer Security, 4*(4), 20-25.

Lisboa, A., Skarmeas, D., & Lages, C. (2011). Entrepreneurial orientation, exploitative and explorative capabilities, and performance outcomes in export markets: A resource-based approach. *Industrial Marketing Management*, *40*(8), 1274-1284.

Locke, E. A. (1968). Towards a theory of task motivation and incentives. *Organizational Behavior and Human Performance, 3*(2), 157-189.

Long, J.S. and L.H. Ervin, 1998. *Correcting for Heteroscedasticity with Heteroscedasticity Consistent Standard Errors in the Linear Regression Model: Small Sample Considerations*. Working Paper. Retrieved from: http://www.indiana.edu/~jslsoc/ research _hccm.htm.

Lumpkin, G. T. & Dess, G. G. (1996). Clarifying the Entrepreneurial Orientation Construct and Linking it to Performance. *Academy of Management Review, 12*(5), 215-234.

Lumpkin, G. T. & Dess, G. G. (2001). Linking two dimensions of entrepreneurial orientation to firm performance: The moderating role of environment and industry life cycle. *Journal of Business Ventures, 16*(3), 429-451.

Lumpkin, G.T. & Sloat, C. (2001). Do Family Firms Have an Entrepreneurial Orientation? *Frontiers of Entrepreneurship Research*, *26*(5), 347-366.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

Madsen E. L. (2007). The significance of sustained entrepreneurial orientation on performance of firms - a longitudinal analysis. *Entrepreneurship and regional Development, 19*(6), 185-204.

Makadok, R. (2001). Towards a Synthesis of the Resource-based and Dynamic-capability Views of Rent Creation. *Strategic Management Journal, 22*(5), 387-401.

Makumbi L., Miriti, E. K., & Kahonge, A. M. (2012). An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector. *International Journal of Computer Applications (IJCA), 57*(18), 33-36.

Manalova, T. S., Brush, C. G., Edelman, L. F. & Greene, P. (2002). Internationalization of small firms: personal factors revisited. *International Small Business Journal, 20*(1), 9-31.

Mark, H. (2003). Application of an improved procedure for testing the linearity of analytical methods to pharmaceutical analysis. *Journal of Pharmaceutical and Biomedical Analysis, 33*(1), 7-20.

Markus, M. L. (1981). Implementation Politics: Top Management Support and User Involvement. *Systems, Objectives, and Solutions*, 203-215.

Martz, E. (2013, 04 16). *Enough is Enough! Handling Multicollinearity in Regression Analysis*. Retrieved 06 14, 2014, from Minitab: http://www.blog.minitab.com.

McAfee, A. & Brynjolfsson, E. (2008, July 24). *Investing in the IT That Makes a Competitive Difference.* Retrieved 06 26, 2013, from HBR: http://hbr.org/.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2011). Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. *Information Systems Management, 28*(2), 102-129.

McGrath, R. G., & MacMillan, I. (2000). *The entrepreneurial mindset*. Boston: Harvard Business School Press.

Mead, D. C. (1998). *Micro and Small Businesses tackle poverty and growth (but in different proportions)*. Paper presented at the conference on Enterprises in Africa: between poverty and growth. Centre for African Studies, University of Edinburgh, 26-27 May.

Melton, C. E., Chen, J. C. H., & Lin, B. (2006). Organisational knowledge and learning: leveraging it to accelerate the creation of competitive advantages. *International Journal of Innovation and Learning, 3*(3), 254-66.

Menguc, B., & Auh, S. (2005). A test of strategic orientation formation versus strategic orientation implementation: the influence of TMT functional diversity and inter-functional coordination. *Journal of Marketing Theory and Practice, 13*(2), 4-19.

Miller, D. (1983). The Correlates of Entrepreneurship in three Types of Firms. *Management Science. 29*(7), 770-791.

Miles, G., Heppard, K. A., Miles, R. E., & Snow, C. C. (2000). *Entrepreneurial strategies: the critical role of top management*. Thousand Oaks, CA: Sage Publications.

Miles, J. & Shevlin, M. (2001). *Applying regression & correlation. A guide for students and researchers*. London: Sage Publications Ltd.

Mills, E. (2009, 01 28). *Study: Cybercrime cost firms $1 trillion globally.* Retrieved 03 01, 2013, from CNET: http://news.cnet.com/8301-1009_3-10152246-83.html.

Montiel-Campos, B., Solé-Parellada, F., Aguilar-Valenzuela, L. A., Berbegal-Mirabent, J., & Duran-Encalada, J. A. (2011). The Impact of Moral Awareness on the Entrepreneurial Orientation-Performance Relationship in New Technology Based Firms. *Journal of Technology Management & Innovation*, 6(4), 93-105.

Montgomery, D. C., Peck, E. A., & Vining, G. G. (2001). *Introduction to Linear Regression Analysis* (3rd ed.). New York: John Wiley.

Moor, S. B., & Manring S. L. (2009). Strategy Development in Small and Medium Sized Enterprises for Sustainability and Increased Value Creation. *Journal of Cleaner Production, 17*(2009), 276-282.

Morris, M. H., Kuratko, D. F., & Covin, J. G. (2008). *Corporate entrepreneurship and innovation*. Cincinnati, OH: Thomson/SouthWestern Publishers.

Morris, M. M., Lewis, P. S. & Sexton, D. L. (1994). Reconceptualizing entrepreneurship: an input-output perspective. *SAM Advanced Management Journal*, Winter, 1-31.

Morris, M. H., & Sexton, D. L. (1996). The concept of entrepreneurial intensity: Implications for company performance. *Journal of Business Research 36*(1), 5-13.

Morris, M. H. (1998). *Entrepreneurial Intensity: Sustainable Advantages for Individuals, Organizations and Societies.* Westport, CT: Quorum Books.

Moss, S. (2009, 04 27). *Fit indices for structural equation modeling.* Retrieved 06 27, 2014, from Psychlopedia: http://www.psych-it.com.au/Psychlopedia/article.asp?id=277.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research Methods: Quantitative & Qualitative Approaches*. Nairobi: Acts Press.

Mugenda, A. (2008). *Social Science Research: Conception, Methodology and Analysis*. Nairobi: Kenya Applied Research and Training Services.

Mureithi, F. (2013, June 10). *Top 100 SMEs search team casts its net wider*. Retrieved August 04, 2013, from BD: http://www.businessdailyafrica.com.

Nichter, S., & Goldmark, L. (2009). Small Firm Growth in Developing Countries. *World Development, 37*(9), 1453-1464.

Njoroge, C. W., & Gathungu, J. M. (2013). The Effect of Entrepreneurial Education and Training on Development of Small and Medium Size Enterprises in Githunguri District-Kenya. *International Journal of Education and Research, 1*(8), 1-22.

Nunnally, J. C. (1978). *Psychometric Theory* (2nd ed.). New York: McGraw-Hill.

Nunnally,J. C. & Bernstein, I. H. (1994). *Psychometric Theory* (3rd ed.). New York: McGraw-Hill.

Ogalo, J. O. (2012). The impact of information system security policies and controls on firm operation enhancement for Kenyan SMEs. *Prime Journal of Business Administration and Management (BAM), 2*(6), 573-581.

Okpara, J. O. (2011). Factors constraining the growth and survival of SMEs in Nigeria Implications for poverty alleviation. *Management Research Review, 34*(2), 156-171.

Olingo, A. (2012, April 18). Internet penetration exposes Kenyans to cybercrime. *The Standard*. Retrieved from http://www.standardmedia.co.ke.

Ong C., & Chen, P. (2013). Information Technology Capability-Enabled Performance, Future Performance, and Value. *Industrial Management & Data Systems, 113*(5), 669-682.

Ong, J. W., & Ismail, H. B. (2008). Sustainable Competitive Advantage through Information Technology Competence: Resource-Based View on Small and Medium Enterprises. *Communications of the IBIMA, 1*(7), 62-70.

Onwubiko, C., & Lenaghan, A. P. (2009). Challenges and complexities of managing information security. *International Journal of Electronic Security and Digital Forensics, 2*(3), 306-321.

Orodho, J. A. (2008). *Techniques of writing research proposals & reports in education and social sciences.* Nairobi: Kanezja HP Enterprises.

Orodho, J. A. (2009). *Elements of education and social science research methods* (2nd ed.). Nairobi: Kanezja HP Enterprises.

Osborne, J. W., Christensen, W. R., & Gunter, J. (2001). *Educational Psychology from a Statistician's Perspective: A Review of the Power and Goodness of Educational Psychology Research.* Paper presented at the national meeting of the American Education Research Association (AERA), Seattle, WA.

Osborne, J. W., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. *Practical Assessment, Research, and Evaluation, 8*(2), 1-5.

Pallant, J. (2010). *SPSS Survival Manual. A step by step guide to data analysis using SPSS* (4th ed.). Melbourne: Open University Press.

Panneerselvam, R. (2006). *Research Methodology*. New Delhi: Prentice-Hall.

Pansuwong, W. (2009). *Entrepreneurial Strategic Orientation and Export Performance of Thai Small and Medium-sized Enterprises*. (Published Doctoral Dissertation, Swinburne University of Technology). Retrieved from http://www.opendoar.org.

Park, C., Jang, S., & Park, Y. (2010). A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance. *IJCSNS International Journal of Computer Science and Network Security, 10*(3), 10-21. Retrieved 02 28, 2013, from http://paper.ijcsns.org/07_book/201003/20100303.pdf.

Park, H. M. (2008). *Univariate Analysis and Normality Test Using SAS, Stata, and SPSS*. Working Paper. The University Information Technology Services (UITS) Center for Statistical and Mathematical Computing, Indiana University.

Patel, V. L., Arocha, J. F. & Shortcliffe, E. H. (2000). Cognitive models in training health professionals to protect patients' confidential information. *International Journal of Medical Informatics, 60*(2), 143-150.

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management and Computer Security, 15*(5), 362-371.

Paul, S. R., & Zhang, X. (2010). Testing for normality in linear regression models. *Journal of Statistical Computation and Simulation, 80*(10), 1101-1113.

Pearl, J. (2000). *Causality: Models, reasoning and inference*. New York: Cambridge University Press.

Pedhazur, E. J. (1997). *Multiple Regression in Behavioral Research* (3rd ed.). Orlando, FL:Harcourt Brace.

Perez-Arostegui, M. N., Benitez-Amado, J., & Tamayo-Torres, J. (2012). Information technology-enabled quality performance: an exploratory study. *Industrial Management & Data Systems, 112*(3), 502-518.

Petti, C., & Zhang, S. (2011). Factors influencing technological entrepreneurship capabilities: Towards an integrated research framework for Chinese enterprises. *Journal of Technology Management in China, 6*(1), 7-25.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.

Ponemon. (2010, 07 24). *2010 Annual Study: U.S. Cost of a Data Breach.* Retrieved 03 01, 2013, from Symantec: http://www.symantec.com/.

.

Poon, J. M. L., Ainuddin, R. A., & Junit, S. H. (2006). Effects of Self-concept Traits and Entrepreneurial Orientation on Firm Performance. *International Small Business Journal, 24*(1), 61-82.

Porter, C. (2012, 04 24). Rising security breaches cost UK plc billions in the last year, shows new PwC/Infosecurity Europe survey. Retrieved 03 01, 2013, from pwc: http://www.ukmediacentre.pwc.com/.

Prahalad, C. K. & Hamel, G. (1990). The core competence of the corporation. *Harvard Business Review, 68*(3), 79-91.

Rastogi, R. (2011). *Information Security Service Management - a service management approach to Information Security Management*. (Published doctoral dissertation, Nelson Mandela Metropolitan University).

Rauch, A., Wiklund, J., Lumpkin, G. T. & Frese, M. (2009). Entrepreneurial orientation and business performance: An assessment of past research and suggestions for the future. *Entrepreneurship Theory Practice*, *33*(9), 761-787.

Ray, G., Muhanna, W. A., & Barney, J. B. (2005). Information Technology and the Performance of the Customer Service Process: A resource-based Analysis. *MIS Quarterly, 29*(4), 625-651.

Reinard, J. (2006). *Communication Research Statistics*. Thousand Oaks, CA: Sage.

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security*, *20*(4), 296-311.

Rezgui, Y. & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers and Security*, *27*, 241-253.

Riani, M., Torti, F., & Zani, S. (2012). *Modern analysis of customer surveys with applications using R.* (1st ed.). Somerset, NJ: John Wiley & Sons.

Richard, F., & Kaplan, S. (2001). *Creative Destruction: Why Companies that Are Built to Last Underperform the Market - and How to Successfully Transform Them.* New York: Currency Books.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods 12*(4), 762–800.

Richard, O. C., Barnett, T., Dwyer, S., & Chadwick, K. (2004). Cultural diversity in management, firm performance, and the moderating role of entrepreneurial orientation dimensions. *Academy of Management Journal*, 47(2), 255-266.

Riddell, K. (2011, 03 08). *Security-Breach Costs Climb 7% to $7.2 Million per Incident.* Retrieved 03 01, 2013, from Bloomberg: http://www.bloomberg.com/.

Rindfleisch, A., Malter, J. A., Ganesan, S., & Moorman, C. (2008). Cross-Sectional versus Longitudinal Survey Research: Concepts, Findings, and Guidelines. *Journal of Marketing Research, 45*(3), 261-279.

Rindskopf, D., & Rose, T. (1988). Some Theory and Applications of Confirmatory Second-order Factor Analysis. *Multivariate Behavioral Research*, 23 (1), 51-67.

Roberts, P. W. (1999). Product innovation, product-market competition and persistent profitability in the US pharmaceutical industry. *Strategic Management Journal, 20*, 655-670.

Rogers, E.M. (1995). *Diffusion of innovations*, (4th ed.). New York: The Free Press.

Ruighaver, A., B., Maynard, S., B. and Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Saad, J. (2013, 02 11). *Faster action against security threats*. Retrieved 03 01, 2013, from smeadvisor: http://www.smeadvisor.com/2013/02/faster-action-against-security-threats/.

Saint-Gemain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-65.

Santhanam, R., & Hartono, E. (2003). Issues in linking information technology capability to firm performance. *MIS Quarterly*, *27*(1), 125-153.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). Harlow: Pearson Education.

Sazali, A. W., Haslinda, A., Jegak, U., & Raduan, C. R. (2009). Moderating Effects of MNCs' Size in the Relationship between Degree of Inter-Firm Technology Transfer and Local Firms' Performance. *American Journal of Scientific Research, 6*(2009), 52-66.

Schaper, M., & Volery, T. (2004). *Entrepreneurship and Small Business: A Pacific Rim Perspective*. Australia: John Wiley & Sons.

Schendel, D. E., & Hitt, M. A. (2007). Issues in Strategic Entrepreneurship. *Strategic Entrepreneurship Journal, 9*(3), 425-453.

Schillo, S. (2011). Entrepreneurial Orientation: What is it and How can it be Useful for Policy and Program Development? *Innovation & Entrepreneurship, 1*(5), 3-7.

Schindehutte, M. & Morris, M. H. (2009). Advancing strategic entrepreneurship research: the role of complexity science in shifting the paradigm. *Entrepreneurship Theory and Practice, 33*(1), 241-276.

Schultz, E. (2004). Security training and awareness - fitting a square peg in a round hole. *Computers & Security, 23*(1), 1-2.

Schumacker, R. E. & Lomax, R. G. (1996). *A Beginner's Guide to Structural Equation Modeling*. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Schumacker, R. E. & Lomax, R. G. (2004). *A Beginner's Guide to Structural Equation Modeling* (2nd ed.). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Schumpeter, J. A. (1934). *The theory of economic development*. Cambridge, MA: Harvard University Press.

Schumpeter, J. A. (1942). *Capitalism, Socialism and Democracy*. New York: Harper & Bros.

Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill building approach* (5th ed.). Somerset, NJ: John Wiley & Sons.

Shamsuddin, S., Othman, J., Shahadan, M. A., & Zakaria, Z. (2012). The Dimensions of Corporate Entrepreneurship and the Performance of Established Organization. *ACRN Journal of Entrepreneurship Perspectives*, *1*(2), 111-131.

Shane, S., & Venkataraman, S. (2000). The promise of entrepreneurship as a field of research. *The Academy of Management Review, 25*, (1), 217-226.

Sharma, N. K., & Dash, P. K. (2012). Effectiveness of ISO 27001 as an information security management system: An analytical study of financial aspects. *Far East Journal of Psychology and Business*, *9*(3), 42-55.

Sharma, R. & Yetton, P. (2006). The contingent Effects of Management Support and task Interdependence on Successful information Systems implementation. *MIS Quarterly, 27*(4), 533-555.

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *VINE: The journal of information and knowledge management systems, 41*(2), 152-166.

Shirokova, G., Vega, G., & Sokolova, L. (2013). Performance of Russian SMEs: exploration, exploitation and strategic entrepreneurship. *Critical perspectives on international business, 9*(1/2), 173-203.

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security*, *17*(4), 296-310.

Siegel, D. S. & Renko, M. (2012). The role of market and technological knowledge in recognizing entrepreneurial opportunities. *Management Decision, 50*(5), 797-816.

Singh, K. (2007). *Quantitative Social Research Methods*. New Delhi: Sage Publications.

Smircich, L. (1992). Organizations as Shared Meanings. In J. M. Shafritz & J. S. Ott (Eds.), *Classics of Organization Theory* (3rd ed.). Pacific Grove, CA: Brooks, Cole Publishing Company.

Smith, A. D. (2004). E-security issues and policy development in an information-sharing and networked environment. *New Information Perspectives, 56*(5), 272-285.

Snedecor, G. W. & Cochran, W. G. (1967). Statistical methods (6th ed.). Ames, Iowa: Iowa State University Press.

Snedecor, G. W. & Cochran, W. G. (1989). *Statistical methods* (8th ed.). Ames, Iowa: Iowa State University Press.

Stam, W., & Elfring, T. (2008). Entrepreneurial orientation and new venture performance: The moderating role of intra- and extraindustry social capital. *Academy of Management Journal, 51*(1), 97-111.

Stebbins, R. A. (2001). *Exploratory Research in the Social Sciences*. Thousand Oaks, CA: Sage Publications.

Stephan, U., & Uhlaner, L. (2010). Performance-based vs socially supportive culture: a cross-national study of descriptive norms and entrepreneurship. *Journal of International Business Studies, 41*(8), 1347-64.

Stevenson, H. H., & Jarillo, J. C. (1990). A paradigm of entrepreneurship: entrepreneurial management. *Strategic Management Journal, 11*, 17-27.

Stockburger, D. W. (2001). *Introductory Statistics: Concepts, Models, and Applications* (2nd ed.). Springfield, USA: Missouri State University Press.

Suhr, D. D. (2006). Exploratory or Confirmatory Factor Analysis? *SUGI 31*(200-31), 1-17.

Sui, G. J., Sheng, M. H., & Song, J. B. (2005). Study on high-tech industrialization based on regional difference of patenting. *Management World, 8*, 87-93.

Symantec. (2013, April 16). *Symantec Internet Security Threat Report Reveals Increase in Cyberespionage - Including Threefold Increase in Small Business Attacks*. Retrieved August 05, 2013, from Symantec: http://www.symantec.com/.

Tabachnick, B. G., & Fidell, L. S. (1989). *Using multivariate statistics*. (2nd ed.). New York: HarperCollins.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics*. (6th ed.). Boston: Pearson.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18,* 509-533.

Tejay, G. P. S., & Barton, K. A. (2013). Information system commitment: A pilot study of external influences on senior management, in *2013 46th Hawaii international conference on system sciences,* 3028-3037.

Thomson, K., & von Solms, R. (2005). Information Security Obedience: A Definition. *Computers & Security, 24*(1), 69-75.

Thoumrungroje, A. (2003). Entrepreneurial Intensity, National Culture and the Success of New Product Developments: The Mediating Role of Information Technology. *AU Journal of Business Management*, 3(1), 15-22.

Trochim, W. M. K. (2006). *Introduction to Validity*. Retrieved 09 09, 2010 from socialresearchmethods: http:// www.socialresearchmethods.net/kb/introval.php.

Upfold, C. T., & Sewry, D. A. (2005). *An Investigation of Information Security in Small And Medium Enterprises (SME's) in the Eastern Cape.* Retrieved 03 06, 2010, from icsa: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082_Article.pdf.

Uzkurt, C., Kumar, R., Kimzan, H. S. & Eminoglu, G. (2013). Role of innovation in the relationship between organizational culture and firm performance: A study of the banking sector in Turkey. *European Journal of Innovation Management, 16*(1), 92 – 117.

Vanhaverbeke, W., Vermeersch, I., & de Zutter, S. (2012). *Open innovation in SMEs: How can small companies and start-ups benefit from open innovation strategies?* Ghent, Belgium: Flandersdc. Retrieved 03 22, 2014, from http://www.flandersdc.be

Venkataraman, S., & Sarasvathy, S. (2001). *Strategy and entrepreneurship: outlines of an untold story* In Hitt, M., Freeman, R. and Harrison, J. (Eds). The Blackwell Handbook of Strategic Management, Blackwell, Oxford, pp. 650-668.

Visintine, V. (2003). *An Introduction to Information Risk Assessment*. Denver, CO: SANS Institute.

Vitale, R., Giglierano, J., & Miles, M. (2003). *Entrepreneurial Orientation, Market Orientation, and Performance in Established and Startup Firms*. Retrieved 08 18, 2014 from cob: http://www.cob.sjsu.edu/facstaff/giglie_j/research/sympap2003.doc.

von Solms, S. H. (2005). Information security governance compliance management vs operational management. *Computers & Security, 24*, 443-447.

Vroom, C. & von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security, 23*(3), 191-198.

Wali, O. P. & Bahl, S. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. *Information Management & Computer Security*, *22*(1), 2-23.

Wall, D. S. (2007). *Cybercrime: The transformation of technology in the networked age*. Cambridge: Polity Press.

Wang, C. L. (2008). Entrepreneurial orientation, learning orientation, and firm performance. *Entrepreneurship: Theory & Practice, 32*(4), 635-657.

Wang, T., & Hsu, C. (2010). *The impact of board structure on information security breaches*. Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Taipei, Taiwan.

Webb, A. R. & Copsey, K. D. (2011). *Statistical pattern recognition* (3rd ed.). Somerset, NJ: John Wiley & Sons.

Whitman, M. E. & Mattord, H. J. (2003). *Principles of Information Security* (1st ed). Boston, MA: Thompson Learning.

Whitman, M. E. & Mattord, H. J. (2005). *Principles of Information Security*. Menlo Park, CA: Thomson Course Technology.

Wiklund, J. (1999). The sustainability of the entrepreneurial orientation-performance relationship. *Entrepreneurship Theory and Practice, 24*(1), 37-48.

Wiklund, J. & Shepherd, D. A. (2003). Knowledge-based resources, entrepreneurial orientation and the performance of small and medium-sized business. *Strategic Management Journal 24*, 1307-1314.

Williams, L. J., Hartman, N., & Cavazotte, F. (2003). *Method variance and marker variables: An integrative approach using structural equation methods*. Paper presented at the Academy of Management, Seattle, WA.

Wright, M. (1999). Third generation risk management practices. *Computers and Security, 1999*(2), 9-12.

Yamane, T. (1967). *Statistics: An Introductory Analysis* (2nd ed.). New York: Harper and Row.

Yeo, A. C., Rahim, M. M., & Miri, L. (2007). Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution. *PACIS 2007 Proceedings*. Paper 74.

Zafar, H., Ko, M., & Osei-Bryson, K. (2012). Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors. *Information Resources Management Journal, 25*(1), 1-28. Retrieved 03 01, 2013, from http://www.igi-global.com/article/financial-impact-information-security-breaches/61419.

Zhang, G., Peng, X., & Li, J. (2008). Technological entrepreneurship and policy environment: a case of China. *Journal of Small Business and Enterprise Development, 15*(4), 733-751.

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2012). *Business Research Methods* (9th ed.). New York: The Free Press.

APPENDICES

APPENDIX I: Letter of Introduction

Date: ………………………….

To ……………………………………………….

…………………………………………………..

…………………………………………………..

Dear Sir/Madam,

RE: <u>COLLECTION OF RESEARCH DATA</u>

I am a student at Jomo Kenyatta University of Agriculture & Technology (JKUAT) pursuing a Ph.D in Entrepreneurship. I am carrying out a research on "*Moderating Role of Entrepreneurial Orientation on the Relationship between Information Security Management and Firm Performance in Kenya*". I am in the process of gathering relevant data for the purpose of this study. You have been identified as one of the collaborators and a key respondent in this study and I would like to kindly invite you to participate in my PhD research. I therefore write to request for your invaluable assistance towards making this study a success by taking time off your busy schedule to respond to the attached questionnaire.

The information collected and used in the PhD Dissertation will be kept strictly confidential, and you will remain completely anonymous throughout data processing. The final report will be made available to you once all analyses are completed. It will be appreciated if you can fill the questionnaire within the next 3 days to enable early finalization of the study. I thank you very much in advance for your consideration, time and responses. Hopefully we can work together to make ISM issues work for us in form of improving the performance of our enterprises.

Yours sincerely,

Stanley Ndung'u

Student Reg. No. HD413-2571/2010; Mob. +254 715 393 904

APPENDIX II: Letter of Authorization

Date: ………………………….

To Executive Director

………………………………………………..

………………………………………………..

NAIROBI

Dear Sir/Madam,

RE: ACADEMIC RESEARCH DATA: "MODERATING ROLE OF ENTREPRENEURIAL ORIENTATION ON THE RELATIONSHIP BETWEEN INFORMATION SECURITY MANAGEMENT AND FIRM PERFORMANCE IN KENYA"

I am a student at Jomo Kenyatta University of Agriculture & Technology (JKUAT) pursuing a Ph.D in Entrepreneurship. I am required to undertake a thesis whose title is as indicated above as partial fulfillment for the award of the doctoral degree. I am kindly requesting for your assistance in making my research a success by granting permission to collect relevant data of your organization from your Head of IT Division. I want to assure your office that all the data collected will be treated with utmost confidentiality and will be used exclusively for the purposes of this academic research.

I am looking forward to your kind consideration and at the same time wishing your esteemed organization success in all her endeavors.

Yours sincerely,

Stanley Ndung'u

Student Reg. No. HD413-2571/2010; Mob. +254 715 393 904

APPENDIX III: Questionnaire

1.0 General Information

This questionnaire is meant to investigate the moderating role of information security management on the performance of small and medium enterprises in Kenya. In particular, it will involve aspects of top management commitment, information security policy enforcement, human-related information security issues (culture, awareness and training), information technology competence, and information security risk assessment.

Note

(a) All responses will be treated in the strictest confidence

(b) If you would like a copy of the findings please supply name and address for receipt of your copy of the findings.

(c) Alternatively, if you would prefer your responses to remain completely anonymous, put only an email address in the address section. Please tick, (√), using copy & paste, where appropriate.

Name:

Address:

Section I: Background Information

(a) Name of your organization (optional) ____

(b) Please specify your sub-sector ____________________________ (e.g. Services or Manufacturing).

(c) How long (years) have you been working as an IT manager in this firm?

□ 0-1 □ 1-5 □ 5-10 □ Over 10

(d) How many people are employed in your organization?

□ 0 - 9 □ 10 - 49 □ 50 – 250

(e) What is your average turnover in KES ‘000,000

□ 0-50 □ 51-100 □ 101-200 □ 201-1,000

Section II: Nature of Information Technology Infrastructure

(a) How many computers do you use in your business? ___________________

(b) Do you make use of Internet in your firm? Yes □ No □

If no, please explain why you do not make use of Internet _________________________________

____

(c) The Internet is used for the following business issues in your organization. Please tick, (√), where appropriate.

No.	**Business Issues**	**Tick (√)**
1	Gathering information on customers	
2	Gathering information on competitors	
3	Establishing a business presence (for instance, website)	
4	Routine communication with customers	
5	Routine communication with suppliers	
6	Providing service / support to customers	
7	Selling services to customers	
8	Others. Please specify.	

Section III: Security Breaches to your Organization

This section consists of statements regarding the approximate number of IT security breaches that your organization has experienced in the last one year. Please respond appropriately by a tick, (√), using the scale provided. Also tick appropriately to indicate the severity of each breach type to your operations.

No.	Breach	Approximate no. of occurrences in the last one year						Severity				
		0	<5	5-10	>10	>100	>1000	Quite Insignificant	Insignificant	Neutral	Significant	Highly Significant
								1	2	3	4	5
1	Damages caused by virus attack											
2	Damages caused by hacking											
3	Physical theft of hardware / software											
4	Computer-based fraud											
5	Damage by displeased employee											
6	Theft, fire or floods											
7	Equipment failure (e.g. hard drive crash)											
8	Other(s)? Please specify below											

Section IV: Top Management Commitment

This section has statements regarding the top management commitment towards ISM in your organization. Please respond as appropriate.

(a) Is information security budgetary allocation in your firm considered as one of the vital components of the overall budget? Yes □ No □

If it is not one of the vital components, please explain ___________________________________

____

(b) Is information security discussed regularly as one of the important agendas in your senior total quality management meetings? Yes □ No □

If not considered as one the important agendas, please explain ____________________________

____

(c) Do employees often complain about security rules? Yes □ No □

If they often do complain, please explain ____

____

(d) Respond with a tick, (√), as appropriate.

No.	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
	Financial Support					
1	Top management gives satisfactory budget allocation to the security program					
2	Top management allocates supplementary/additional budget to the security program when need arises					
	Management Participation					
3	Top management participation is a signal to other employees of how to value information security initiatives					
4	The results of information security evaluation are reviewed with staff and reported to the board of directors					
5	Top management is always willing to learn and to be informed on vital information security issues					
	User Satisfaction					
6	User satisfaction represents the success of various managerial interventions designed to promote end-user adoption					
7	Employees value the importance of security					
8	Any other? Please specify below					

Section V: Information Security Policy Enforcement

This section has statements regarding information security policy enforcement in your organization. Kindly respond as appropriate.

(a) Are Information security policies written in a manner that is clear and understandable?

Yes □ No □

If not written in a clear and understandable manner, please explain ________________________

____

(b) Are necessary efforts made to educate new employees about current security policies?

Yes □ No □

If necessary efforts not made, please explain ____

____

(c) Have employees been trained to regard Information Security Policies as the main tool for achievement of Information Security Management activities? Yes □ No □

If not trained this in this regard, please explain ____

____

(d) Does your firm encourage interdepartmental discussions in regard to updating and improving security policies? Yes □ No □

If discussions not encouraged, please explain ____

____

(e) Respond with a tick, (√), as appropriate.

No.	**Statement**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
		1	2	3	4	5
	Right Implementation					
1	Information security policies are rightly implemented such that cases of manipulation are unheard of					
2	An established information security policy review and update process exists					
3	Information security policies are aligned with business goals					
	Acceptance by Employees					
4	Your firm is successful because when a policy is created it receives acceptance by employees					
5	Effective security monitoring is emphasized in your firm in order to enforce security control policies					
	Teamwork					
6	Teamwork is encouraged because everyone is affected by information security to some extent					
7	Information security is a key norm shared by organizational members					
8	Any other? Please specify below.					

Section VI: Human-related information security issues (culture, awareness and training)

This section has statements regarding human-related information security issues (culture, awareness and training) in your organization. Kindly respond with as appropriate.

(a) Is information security culture embedded in your organizational culture? Yes □ No □

If not embedded, please explain ____

____

(b) Does your organization use training and awareness programs to enhance and make easier, implementation of information security? Yes □ No □

If training and awareness programs not used as above, please explain ______________________

____

(c) Do users receive adequate security training prior to getting a network account?

Yes □ No □

If not, please explain ____

____

(d) Kindly respond with a tick, (√), as appropriate.

No.	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
	Culture					
1	Your organization makes security part of the way you do business, your operational culture					
2	The influence and guidance of your management fosters a positive attitude of security					
	Awareness					
3	Raising security awareness is an activity that is given an important priority					
	Training					
4	To achieve the required outcome from the implementation of an information security your organization insists on an on-going regular and structured training and awareness program					
5	Users receive adequate security refresher training appropriate for their job function					
6	Any other? Please specify below.					

Section VII: Information Technology Competence

This section has statements regarding IT competence in your organization. Kindly respond as appropriate.

(a) Have your members of staff been trained to secure their computers at all times, when moving away from their work stations, e.g. locking or logging off their computers, when going for a tea break or out to lunch, e.tc.? Yes □ No □

If not trained along those lines, please explain ____

____

(b) Are your members of staff that travel with portable computers in your firm aware of the risk relating to theft and the potential liability through compromised data? Yes □ No □

If no, please explain ____

____

(c) Despite being connected to public networks, are you confident that your systems are adequately protected? Yes □ No □

If not adequately protected, please explain ____

____

(d) Kindly respond with a tick, (√), as appropriate.

No.	**Statement**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
		1	2	3	4	5
	Knowledge of Information Systems					
1	Expertise on information security is available internally, and where not, your firm seeks external advice					
2	Your staff know what to do with information with regard to its storage, usage, archiving, backup and destruction					
	Experience in Information Systems					
3	All your systems provide audit trails					

4	Roles and responsibilities for information security in your organization are well defined					
5	You are confident of technological competence invested in your team over time					
	Information Systems Resources					
6	Information Systems resources are adequate, well maintained and/or replaced as appropriate					
7	Information Systems resources are in synchronization with technological advancements					
8	Any other? Please specify below.					

Section VIII: Information security risk assessment

This section has statements regarding information security risk assessment in your organization. Kindly respond as appropriate.

(a) Does risk assessment in your firm determine what the consequences would be if the infrastructure became inoperable? Yes □ No □

If no, please explain ____

____

(b) Does risk assessment in your organization consider what information assets are subject to laws and regulations and that the assessment results in adequate procedures to assure compliance? Yes □ No □

If no, please explain ____

____

(c) Does your organization make security and risk assessment part of the way you do business?

Yes □ No □

If no, please explain ____

____

(d) Kindly respond with a tick, (√), as appropriate.

No.	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
	Threats & Vulnerabilities					
1	Your organization has in place an adequate risk assessment process					
2	Your organization employs one of the popular ISRA methodologies					
3	Your staff are trained towards mitigating threats and vulnerabilities					
	Potential Impact					
4	Your organization rates each risk according to potential impact					
5	Risk assessment in your firm cover the consequences of a security incident in terms of lost revenues, lost customers and investor confidence					
	Likelihood of Occurrence					
6	Risk assessment considers whether the entity can continue to operate if critical information is unavailable, compromised or lost					
7	Your organization rates each risk according to likelihood of occurrence					
8	Any other? Please specify below.					

Section IX: Entrepreneurial Orientation

(i) This section has statements regarding entrepreneurial orientation in your organization. Kindly respond with a tick, (√), as appropriate.

(a) Does your organization re-engineer your processes to make them more efficient than your competitors' processes? Yes □ No □

If your organization does not re-engineer your processes, please explain ____________________

____

(b) Does your organization create partnerships with the best partners in the industry before competitors enlist them? Yes □ No □

If no, please explain ____

____

(c) If a manager takes a risk and fails, does your firm punish him / her? Yes □ No □

If no punishment is meted, please explain ____

____

(d) Kindly respond with a tick, (√), as appropriate.

No.	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
	Innovating					
1	Your organization creates new products that will provide value to new or existing customers					
2	Your organization finds non-product ways to create value for new or existing customer, such as through distribution, advertising, or other communications					
	Acting Proactively					
3	Your organization beats competitors to enter new markets					
4	Your organization introduces new products or services before your competitors do					
5	Your organization improves the quality or the number of features of your products or services before your competitors do, and prices proactively					
	Managing Risks					
6	Your firm takes the risk of missing an opportunity with the same weight as the risk of failure					
7	In order to make effective changes to your offering, your firm is willing to accept at least a moderate level of risk of significant losses					
8	Any other? Please specify below.					

(ii) Kindly indicate the average growth for the indicators of performance in your firm, from 2010 to 2012. If an indicator experienced a growth of, say, 20% in a particular year, indicate 120%. If it declined with a certain percentage, for instance, 30%, indicate 70%. The profitability trend will be partly indicative of effectiveness of information security management adoption.

Profitability Ratio	**2010**	**2011**	**2012**
Average Pre-tax Profits			
Return on Equity (ROE)			
Return on Assets (ROA)			
Employment Growth			
Sales Turnover			

(a) Has information security management played any role in your profitability improvement?

Yes □ No □

If yes, please indicate by what percentage, using a tick, (√), as appropriate.

□ 1-5%
□ 6-10%
□ 11-15%
□ 16-20%
□ Over 21%

I want to thank you most sincerely for affording time, out of your very busy schedule, to respond to the research questionnaire.

APPENDIX IV: List of Medium-sized Firms in the 2013 Top 100 Survey

Rank in 2013 Top 100 Survey	Name of Company
1	LEAN ENERGY SOLUTIONS LTD.
2	EAST AFRICAN CANVAS CO. LTD
3	DIGITAL CITY LTD
4	PLENSER LTD
5	ALLWIN AGENCIES (K) LTD
6	PROPACK KENYA LTD
7	VIVEK INVESTMENTS LTD
8	POWERPOINT SYSTEMS (EA) LTD
9	CONINX INDUSTRIES LTD.
10	SYNERMEDICA PHARMACEUTICALS (KENYA) LTD
11	COAST INDUSTRIALS & SAFETY SUPPLIES LTD
12	ISOLUTIONS ASSOCIATES
13	WOTECH KENYA LIMITED
14	AVTECH SYSTEMS LIMITED
15	KENYA BUS SERVICE
16	MURANGA FORWARDERS
17	SYNERMED PHARMACEUTICALS (K) LTD
18	TISSUE KENYA LTD
19	KENYA HIGHLAND SEED CO LTD
20	FAMIAR GENERATING SYS LTD
21	ALEXANDER FORBES
22	CHEMICALS & SCHOOL SUPPLIES LTD.
23	CHARLSTONE TRAVEL LIMITED
24	ONFON MEDIA LTD
25	ELITE TOOLS LTD
26	EUROCON TILES PRODUCTS LTD
27	ENDEVOUR AFRICA LIMITED
28	RONGAI WORKSHOP & TRANSPORT LTD
29	R & R PLASTICS LTD
30	CHIGWELL HOLDINGS LTD
31	CLASSIC MOULDINGS LIMITED
32	PEWIN CABS LIMITED
33	NOVEL TECHNOLOGIES EA LTD
34	XTREME ADVENTURES LTD
35	VINTAGE AFRICA LIMITED
36	PUNJANI ELECTRICAL & INDUSTRIAL HARDWARE LTD

37	SPRY ENGINEERING CO. LTD
38	GENERAL CARGO SERVICES LTD
39	PINNACLE (K) TRAVEL & SAFARIS
40	PANESARS KENYA LIMITED
41	SPECIALIZED ALUMINIUM RENOVATORS LTD.
42	CUBE MOVERS LIMITED
43	BROGIIBRO COMPANY LTD
44	TOTAL SOLUTIONS LTD
45	TYREMASTERS LTD
46	XRX TECHNOLOGIES LIMITED
47	SENSATION LTD
48	EUREKA TECHNICAL SERVICES LTD
49	PALBINA TRAVEL LIMITED
50	WAUMINI INSURANCE BROKERS LTD
51	ASL CREDIT LIMITED
52	ZAVERCHAND PUNJA LIMITED
53	CANON CHEMICALS LTD
54	PACKAGING MANUFACTURERS(1976) LTD
55	TRIDENT PLUMBERS LTD
56	TYPOTECH
57	KINPASH ENTERPRISES LTD
58	VEHICLE & EQUIPMENT LEASING LTD
59	SHEFFIELD STEEL SYSTEMS
60	COMPLAST INDUSTRIES LTD
61	DUNE PACKAGING LIMITED
62	HEBATULLAH BROTHERS LIMITED
63	SPICE WORLD LIMITED
64	MUSEUM HILL WINES LTD
65	YOGI PLUMBERS LTD
66	VAJRA DRILL LTD
67	MELVN MARSH INTERNATIONAL LTD
68	KANDIAFRESH PRODUCE SUPPLIERS LTD
69	FAYAZ BAKERS LIMITED
70	SPECICOM TECHNOLOGIES LIMITED
71	MOMBASA CANVAS LTD
72	SILVERBIRDTRAVEL PLUS LTD
73	IRON ART
74	RADAR LIMITED
75	MASTER POWER SYSTEMS
76	HARDWARE & WELDING SUPPLIES

77	MASTERS FABRICATORS LTD
78	SOFTWARE TECHNOLOGIES LTD
79	HERITAGE FOODS KENYA LTD
80	AFRICA TEA BROKERS LTD
81	RAEREX (EA) LIMITED
82	TRAVELSHOPPE COMPANY LTD
83	ORIENTAL GENERAL STORES LTD
84	CHUMA FABRICATORS LTD
85	STATPRINT LTD
86	SOLLATEK ELECTRONICS LTD
87	SMARTBRANDS LTD
88	DE RUITER EAST AFRICA LTD
89	KISIMA DRILLING (EA) LTD
90	CARE CHEMISTS
91	BROLLO KENYA LTD
92	CANON ALUMINIUM FABRICATORS LTD
93	SATGURU TRAVEL & TOURS LTD
94	KUNAL HARDWARE AND STEEL
95	DEEPA INDUSTRIES LIMITED
96	SKYLARK CREATIVE PRODUCTS LTD.
97	UNEEK FREIGHT SERVICES LTD
98	BBC AUTO SPARES LTD
99	LANTECH (AFRICA) LIMITED.
100	POLYTANKS LIMITED

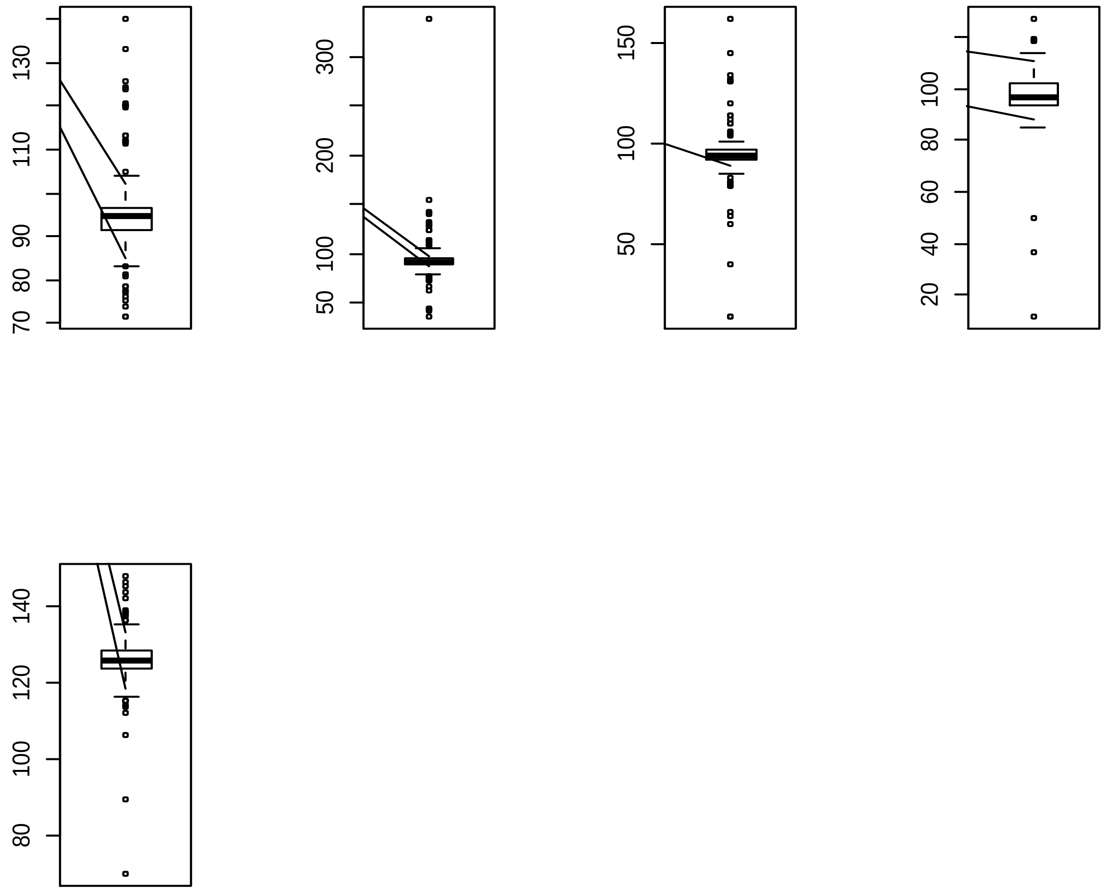
APPENDIX V: Description of Factors of the Study Variables

Item	Descriptions	Construct (Informative & Reflective)
TMC1	Top management gives satisfactory budget allocation to the security program	**Top Management Commitment (TMC)**
TMC2	Top management allocates supplementary/additional budget to the security program when need arises	
TMC3	Top management participation is a signal to other employees of how to value information security initiatives	
TMC4	The results of information security evaluation are reviewed with staff and reported to the board of directors	
TMC5	Top management is always willing to learn and to be informed on vital information security issues	
TMC6	User satisfaction represents the success of various managerial interventions designed to promote end-user adoption	
TMC7	Employees value the importance of security	
ISE1	Information security policies are rightly implemented such that cases of manipulation are unheard of	**Information Security Policy Enforcement (ISPE)**
ISE2	An established information security policy review and update process exists	
ISE3	Information security policies are aligned with business goals	
ISE4	Your firm is successful because when a policy is created it receives acceptance by employees	
ISE5	Effective security monitoring is emphasized in your firm in order to enforce security control policies	
ISE6	Teamwork is encouraged because everyone is affected by information security to some extent	
ISE7	Information security is a key norm shared by organizational members	
HRI1	Your organization makes security part of the way you do business, your operational culture	**Human-related information security issues (HRI)**

Item	Descriptions	Construct (Informative & Reflective)
HRI2	The influence and guidance of your management fosters a positive attitude of security	
HRI3	Raising security awareness is an activity that is given an important priority	
HRI4	To achieve the required outcome from the implementation of an information security your organization insists on an on-going regular and structured training and awareness program	
HRI5	Users receive adequate security refresher training appropriate for their job function	
ITC1	Expertise on information security is available internally, and where not, your firm seeks external advice	**Information Technology Competence (ITC)**
ITC2	Your staff know what to do with information with regard to its storage, usage, archiving, backup and destruction	
ITC3	All your systems provide audit trails	
ITC4	Roles and responsibilities for information security in your organization are well defined	
ITC5	You are confident of technological competence invested in your team over time	
ITC6	Information Systems resources are adequate, well maintained and/or replaced as appropriate	
ITC7	Information Systems resources are in synchronization with technological advancements	
RSR1	Your organization has in place an adequate risk assessment process	**Information security risk assessment (ISRA)**
RSR2	Your organization employs one of the popular ISRA methodologies	
RSR3	Your staff are trained towards mitigating threats and vulnerabilities	
RSR4	Your organization rates each risk according to potential impact	
RSR5	Risk assessment in your firm cover the consequences of a security incident in terms of lost revenues, lost customers and investor confidence	

Item	Descriptions	Construct (Informative & Reflective)
RSR6	Risk assessment considers whether the entity can continue to operate if critical information is unavailable, compromised or lost	
RSR7	Your organization rates each risk according to likelihood of occurrence	
EO1	Your organization creates new products that will provide value to new or existing customers	**Entrepreneurial Orientation (EO)**
EO2	Your organization finds non-product ways to create value for new or existing customer, such as through distribution, advertising, or other communications	
EO3	Your organization beats competitors to enter new markets	
EO4	Your organization introduces new products or services before your competitors do	
EO5	Your organization improves the quality or the number of features of your products or services before your competitors do, and prices proactively	
EO6	In order to make effective changes to your offering, your firm is willing to accept at least a moderate level of risk of significant losses	
EO7	Your firm takes the risk of missing an opportunity with the same weight as the risk of failure	
PR1	Average Pre-tax Profits	**Firm Performance (FP)**
PR2	Return on Equity (ROE)	
PR3	Return on Assets (ROA)	
PR4	Employment Growth	
PR5	Sales Turnover	

APPENDIX VI Testing of Outliers on the Dependent Variable



APPENDIX VII: Testing of Normality (Skewness and Kurtosis)

Main Construct	Factors	Mean	SE (±µ)	Std.	Skewness	Kurtosis	3xSkewness	3xkurtosis
Top Management Commitment (TMC)	TMC1	3.7	0.1	0.9	-1.9	3.6	0.3	0.3
	TMC2	3.9	0.1	0.7	-2.2	7.2	0.2	0.2
	TMC3	3.9	0.1	0.5	**-1.2**	3.3	0.2	0.2
	TMC4	3.6	0.1	0.9	-1.5	1.9	0.3	0.3
	TMC5	3.8	0.1	0.8	-2.1	5.3	0.2	0.2
	TMC6	4.0	0.1	0.6	-1.8	7.6	0.2	0.2
	TMC7	4.0	0.1	0.7	-1.9	7.0	0.2	0.2
Information Security Policy Enforcement (ISPE)	ISE1	3.9	0.1	0.7	-2.3	7.9	0.2	0.2
	ISE2	3.7	0.1	0.8	-1.6	2.3	0.2	0.2
	ISE3	3.9	0.1	0.7	-2.0	7.3	0.2	0.2
	ISE4	3.9	0.1	0.6	-2.1	8.0	0.2	0.2
	ISE5	3.9	0.1	0.7	-2.1	7.9	0.2	0.2
	ISE6	4.0	0.1	0.7	-2.1	7.8	0.2	0.2
	ISE7	3.9	0.1	0.6	-2.4	9.4	0.2	0.2
Human-related information security issues (HRI)	HRI1	3.8	0.1	0.7	-1.9	6.3	0.2	0.2
	HRI2	3.8	0.1	0.7	-2.4	7.5	0.2	0.2
	HRI3	3.9	0.1	0.7	-1.9	5.7	0.2	0.2
	HRI4	3.8	0.1	0.7	-1.7	4.5	0.2	0.2
	HRI5	3.8	0.1	0.7	-1.7	4.4	0.2	0.2
Information Technology Competence (ITC)	ITC1	4.2	0.1	0.7	-2.0	9.1	0.2	0.2
	ITC2	4.3	0.1	0.6	-1.3	5.8	0.2	0.2
	ITC3	3.6	0.1	0.9	**-0.6**	**0.0**	0.3	0.3
	ITC4	4.0	0.1	0.8	-1.7	5.3	0.2	0.2
	ITC5	4.2	0.1	0.7	-1.4	4.2	0.2	0.2
	ITC6	4.0	0.1	0.7	-1.3	4.9	0.2	0.2
	ITC7	3.7	0.1	0.7	**-1.0**	1.9	0.2	0.2
Information security risk assessment (ISRA)	RSR1	3.7	0.1	0.7	-2.1	5.0	0.2	0.2
	RSR2	2.7	0.1	0.7	**-0.1**	-1.5	0.4	0.4
	RSR3	3.8	0.1	0.7	-1.7	3.3	0.2	0.2
	RSR4	3.9	0.1	0.7	-1.7	4.2	0.2	0.2

Main Construct	Factors	Mean	SE (±µ)	Std.	Skewness	Kurtosis	3xSkewness	3xkurtosis
	RSR5	3.8	0.1	0.7	-1.8	4.2	0.2	0.2
	RSR6	3.8	0.1	0.7	-2.3	7.1	0.2	0.2
	RSR7	3.8	0.1	0.6	-2.5	7.5	0.2	0.2
Entrepreneurial Orientation (EO)	EO1	4.2	0.1	0.6	-1.5	11.0	0.2	0.2
	EO2	4.2	0.1	0.7	-1.4	9.1	0.2	0.2
	EO3	4.1	0.1	0.6	**-1.0**	3.4	0.2	0.2
	EO4	4.1	0.1	0.6	**-1.2**	5.8	0.2	0.2
	EO5	4.1	0.1	0.7	-1.3	7.7	0.2	0.2
	EO6	3.9	0.1	0.7	-1.2	4.2	0.2	0.2
	EO7	4.0	0.1	0.7	-2.3	7.9	0.2	0.2
Profitability Ratio (PR)	PR1	96.3	1.4	13.2	**0.9**	1.3	4.1	4.1
	PR2	95.5	3.2	30.9	**5.2**	40.4	9.6	9.6
	PR3	94.1	2.1	20.1	**-0.8**	6.3	6.2	6.2
	PR4	96.9	1.5	14.7	-3.0	15.3	4.5	4.5
	PR5	125.6	1.0	10.1	-2.0	10.8	3.1	3.1

APPENDIX VIII: Communality Values to Measure Variability of Observed Variables

	Communalities	
Main Factor	**Items**	**Extraction**
Profitability Ratio (PR)	PR1	.791
	PR2	.611
	PR3	.824
	PR4	.751
	PR5	.779
Entrepreneurial Orientation (EO)	EO1	.833
	EO2	.870
	EO3	.859
	EO4	.903
	EO5	.870
	EO6	.896
	EO7	.899
Human-related information security issues (HRI)	HRI1	.874
	HRI2	.898
	HRI3	.940
	HRI4	.854
	HRI5	.885
Information Security Policy Enforcement (ISPE)	ISE1	.812
	ISE2	.808
	ISE3	.826
	ISE4	.746
	ISE5	.813
	ISE6	.880
	ISE7	.726
Information security risk assessment (ISRA)	RSR1	.833
	RSR2	.870
	RSR3	.859
	RSR4	.903
	RSR5	.870
	RSR6	.896
	RSR7	.899

	Communalities	
Main Factor	Items	Extraction
Top Management Commitment (TMC)	TMC 1	.631
	TMC 2	.713
	TMC 3	.796
	TMC 4	.733
	TMC 5	.816
	TMC 6	.679
	TMC 7	.731
Information Technology Competence (ITC)	ITC1	.874
	ITC2	.898
	ITC3	.940
	ITC4	.854
	ITC5	.885
	ITC6	.794
	ITC7	.837

APPENDIX IX Extracted Components Obtained by Constraining Factors

	Initial Eigenvalues			**Extraction Sums of Squared Loadings**		
Item	**Total**	**% of Variance**	**Cumulative %**	**Total**	**% of Variance**	**Cumulative %**
1	17.79	39.53	39.53	17.790	39.532	39.532
2	5.39	11.97	51.50	5.386	11.969	51.501
3	2.83	6.29	57.79	2.829	6.288	57.789
4	2.32	5.16	62.95	2.322	5.160	62.949
5	1.99	4.41	67.36	1.986	4.413	67.362
6	1.77	3.92	71.29	1.766	3.924	71.286
7	1.62	3.59	74.88	1.617	3.593	**74.880**
8	1.36	3.02	77.90			
9	1.15	2.56	80.46			
10	1.05	2.33	82.79			
11	0.82	1.83	84.62			
12	0.80	1.77	86.40			
13	0.75	1.68	88.08			
14	0.70	1.55	89.63			
15	0.59	1.31	90.93			
16	0.55	1.21	92.15			
17	0.46	1.03	93.17			
18	0.41	0.92	94.10			
19	0.37	0.81	94.91			
20	0.32	0.71	95.62			
21	0.30	0.66	96.28			
22	0.27	0.59	96.87			
23	0.24	0.54	97.41			
24	0.21	0.47	97.88			
25	0.20	0.44	98.32			
26	0.18	0.39	98.71			
27	0.16	0.35	99.06			
28	0.13	0.29	99.35			
29	0.10	0.23	99.59			
30	0.06	0.14	99.72			

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Item	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
31	0.05	0.12	99.84			
32	0.04	0.09	99.93			
33	0.03	0.07	100.00			
34	0.00	0.00	100.00			
35	0.00	0.00	100.00			
36	0.00	0.00	100.00			
37	0.00	0.00	100.00			
38	0.00	0.00	100.00			
39	0.00	0.00	100.00			
40	0.00	0.00	100.00			
41	0.00	0.00	100.00			
42	0.00	0.00	100.00			
43	0.00	0.00	100.00			
44	0.00	0.00	100.00			
45	0.00	0.00	100.00			

APPENDIX X Reliability Test

Retained Factors	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted	Overall Cronbach's Alpha
EO3	.659	.808	.867
EO4	.775	.784	
EO5	.695	.812	
EO7	.287	.912	
HRI2	.491	.692	0.761
HRI4	.439	.654	
HRI5	.559	.651	
ISE3	.629	.851	0.891
ISE4	.547	.890	
ISE6	.799	.809	
ISE7	.651	.880	
ITC2	.491	.755	0.817
ITC4	.392	.810	
ITC5	.557	.677	
PR1	.647	.418	0.731
PR4	.647	.418	
RSR3	.659	.808	0.867
RSR4	.775	.784	
RSR5	.695	.812	
RSR7	.287	.912	
TMC 4	.530	.811	0.881
TMC 5	.635	.716	
TMC 7	.488	.837	