INFORMATION TECHNOLOGY SECURITY PRACTICES AND PERFORMANCE OF SMALL AND MEDIUM ENTERPRISES IN NAIROBI COUNTY, KENYA

GLADWELL NJOKI MURIGI

D53/OL/CTY/24562/2014

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF BUSINESS IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF BUSINESS ADMINISTRATION DEGREE (MANAGEMENT INFORMATION SYSTEM OPTION) OF KENYATTA UNIVERSITY

MAY, 2017

DECLARATION

I hereby declare that this project is my original work and has not been presented to any University or Tertiary Institution for examination / assessment.

Signature……Date……..

Gladwell Njoki Murigi

D53/OL/CTY/24562/2014

Kenyatta University

This research project has been presented for examination with my approval as the appointed University Supervisor.

Signature……. Date……

Ms. Gladys Kimutai

Lecturer, Department of Management Science

Kenyatta University

ACKNOWLEDGEMENT

It was not possible to undertake this proposal without seeking help from others. First and foremost, I acknowledge the peace of God which surpasses all human understanding. My deep and sincere thanks go to my supervisor, Ms. Gladys Kimutai, my advisor and to all my lecturers in the School of Business for their suggestions, supervision and direction in the preparation of this research project. I also take his opportunity to thank my family supporting and understanding me as I had set aside some of my family responsibilities to work on this project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

GDP:	Gross Domestic Product
GDT:	General Deterrence Theory
GoK:	Government of Kenya
ICT:	Information Communication and Technology
IS:	Information System
ISS:	Information Systems Security
IT:	Information Technology
NCBDA:	Nairobi Central Business District Association
PWC:	Price Water-House Coopers
ROA:	Return on Assets
ROE:	Return on Equity
SETA:	Security Education, Training, and Awareness
SMEs:	Small and Medium Enterprises
SQL:	Structured Query Language
UK:	United Kingdom
UN:	United Nations
USA:	United States of America

DEFINITION OF TERMS

Information Technology Policies:	They define common processes, procedures, roles and responsibilities should be followed by employees within an organization
Awareness:	This refers to creation of a sense of familiarity so that an individual be able to carry out their tasks with the required knowledge
Training:	These are strategies that develop, maintain, and improve the operational readiness of individuals or units within the organization
Performance:	This is the alignments of business units in an organization with an aim of ensuring the organization's goals are met in terms of sales volume, profitability and customer satisfaction
System Monitoring and Maintenance:	Planning and executing processes such as testing, repairing and other minor modifications that will result in improved functionality
Access control:	This is selective restriction to an area. Access is granted upon verification.

ABSTRACT

Small and medium enterprises are major stakeholders in developing countries economies. In Kenya although SMEs take off on a high note their life span is short. SMEs are more exposed to information security risks, short life and thus poor performance. The general objective of this study was to investigate the on the influence of information technology security practices on the performance of small and medium enterprises in Nairobi County. This research study used a descriptive research design. The targeted population was the 1,221 owners or general managers of all the SMEs in the hotel sector operating in Nairobi County. Random sampling was used to choose a sample size of 292 SME owners or managers from the targeted population. Semi structured questionnaires were used to collect primary data. To test the reliability and validity of the instruments of research a pilot test was conducted. Thematic content analysis was used to analyze qualitative data realized from open-ended questions while quantitative data was analyzed using inferential and descriptive statics by employing Statistical Package for Social Sciences (SPSS version 22). Descriptive statistics and multiple regression analysis were employed to determine the relationship between independent and dependent variables. The study found that privacy and confidentiality policy, back up policy as well as policies on sharing, storing and transmitting of data influence the performance of SMEs in Kenya. In addition, communication channels, security training and education as well as frequency of training influences the performance of SMEs in Kenya. The study established that use of passwords was the most used access control measure to enhance information technology security, followed by smart cards and biometric access controls. The study recommends that SMEs that have adopted information technology to come up with an IT security policies. The policies should comprise of use of passwords, encryption and consequences of misuse of ICT resources among others. In addition, the management of SMEs should plan for training programs on information technology security. This will help in ensuring that the staff have up-to-date information on security risks and how to mitigate them.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

In the current stiff and tough business environment, business organizations such as small and medium enterprises require information systems to track their business activities, right from business planning to product or service delivery. Due to huge order-turnovers, tracking the number of resources in an organization and monitoring the overall business performance has in the recent past become a challenge to many organizations. This has resulted in the adoption of technology which has been a challenging activity to many SMEs in this era. This is as a result of the increasing competitive markets, increasing supply chain dependency and increasing need to improve the customer base (Casaca, 2014).

Information systems (IS), Information Communication technologies (ICT) and the vast use of the Internet has enabled organizations to rely on computers as media for creating, processing, managing and transmitting sensitive business information. However, this use of IS / ICT and the Internet at large exposes the information assets to attacks, flaws and vulnerabilities, ranging from computer frauds, espionage, sabotage, and vandalism to other incidents, such as fire or floods. The risks are identical for both big firms and for SMEs . Beachboard , (2008).

SMEs are more exposed to these risks because of their restricted financial and human capacity which is required to develop and employ strong security programs. One of the important assets of SMEs is knowledge and its loss can cause dire consequences to SMEs thus there is need to secure their information assets away from internal and external threats (Casaca, 2014).

1.1.1 Information Technology Security Practices

A positive information security culture enhances information security as it can aid in reducing the people threat when working with IT systems (Ngura, Kimwele & Rotich, 2015). Highlighting the importance of information security risks are recent numbers from Australia, USA and UK, which indicate that the abuse and misuse of the internet by employees gives rise to 50 percent of internet incidents. Owing to this finding, a survey in Australia found out that 40 percent of the interviewed companies pointed out information security as a main point of concern (AusCert, 2005). Employees unintentionally trigger information security risks e.g. by unknowingly accepting spam emails, downloading virus containing attachments or simply ignoring information security warnings (Besnard and Arief 2004).

An article titled "threat within" by McAfee (2005), indicated that; 21 percent of workers permitted friends and family to use company personal computers and laptops to access the internet; 51 percent connected their devices such as phones and flash disks to the company PCs, 60 percent stored personal information on the company computers while 10 percent downloaded prohibited material at the work place. This results in high exposure of the company information to risk.

Glibly, Upfold and Sewry (2008) carried out an investigation of information security in small and medium enterprises (SME's) in the Eastern Cape. The study used a survey research design. The results of the survey 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, 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.

According to ISACA (2009) due to the popularity of electronic commerce, many organizations are facing security challenges. Enterprises too often view information security in isolation: the perception is that security is someone else's responsibility and there is no collaborative effort to link the security program to business goals. This leads to weaknesses in security management which results in serious exposure.

In Kenya, a firm with ten or less workers is known as a micro-enterprise, while those with between ten to fifty workers are called small enterprises. Medium enterprises consist of 51 employees to a hundred workers. According to GoK, enterprises with between one and fifty employees are defined as SMEs whether informal or formal. SME growth can be enhanced by adapting Information Communication Technology (ICT). SME evolution in relation to information security relies on the use of ICT. The protection of information in an organization as well as protection of the hardware and systems used to store, manufacture and send this information is known as Information Security (Casaca, 2014).

Over the last several decades, managers have become alive to the fact that information systems and information are vital organizational resources (Mochoge, 2013). Ngura, Kimwele and Rotich (2015), state that data security is vital to a firm's operation. When data is not properly stored, manufactured and relayed, operations will be affected and thus resulting in serious effects to trading.

1.1.2 Small and Medium Enterprises in Nairobi County

Nairobi County is home to Nairobi city, Kenya's capital. Nairobi is Kenya's main administrative, economic and cultural hub and one of Africa's fastest growing urban center. Being the Kenyan capital, Nairobi County is home to about 60 percent of the SMEs in Kenya which straddle across

various sectors ranging from the informal sector, banking, retail, farming among others (Krop, 2014).

It is estimated that Nairobi County hosts 5 million micro and small scale traders offering employment to 8 million people. According to Nairobi County government as cited by Mochoge (2014), there are 30,252 registered SMEs in Nairobi County. Analysis by county shows that Nairobi County recorded a 5.4 percent increase in job creation in 2011 in the SMEs sector (ROK, 2012). Like in any other part of the country SMEs in Nairobi have a short life span and do not go beyond the third anniversary (ROK, 2012).

1.2 Statement of the Problem

SMEs play a major role in the economy of developing countries. In the year 2012, SMEs contributed about 70 percent to the country's GDP. In addition, the SME sector in Kenya generates over 80 percent of the Nation's work force with many of the new jobs originating from this sector (GoK, 2012).

According to Sharu and Guyo (2015), small and medium enterprises in Kenya have a short life span and face major hurdles resulting to 60 percent performance failures within the initial three years from inception. According to Ngura, Kimwele and Rotich (2015) SMEs are more exposed to information security risks. Consequently, a United Nations (UN) report stated that this exposure to risks results in poor performance and a high mortality rate. High mortality rate for the SMEs leads to unemployment and thus reduced economic development for a nation (GoK, 2013)

With all this risks, SMEs still have not been able to implement measures to avoid these risks. Beachboard (2008) noted that security risk management is uncommon and training in many

organizations is not thorough due to inadequate support from the management. This shows that there is still a lot that needs to be done in order to secure information held by Kenyan SMEs.

In Portugal, Casaca (2014) conducted a study on what determines effectiveness of the information security in small and medium sized enterprises. In Europe and USA, Dimopoulos (2014) conducted a study on the approaches of information technology security among SMEs. In Kenya, Mochoge (2013) did a study on the factors affecting the implementation of strategic information systems among small and medium companies. However, despite the immense enquiry into information security, none of these studies has been done to analyze information technology security practices in small and medium enterprises. This study was aimed at filling this gap by investigating the influence of information technology security practices on performance of small and medium enterprises in Nairobi County.

1.3 Objectives of the Study

1.3.1 General Objective

The general objective of this study was to investigate on the influence Information Technology Security Practices on performance of small and medium enterprises in Nairobi County.

1.3.2 Specific Objectives

The specific objective of this study was:

i. To establish how information technology policies influence the performance of small and medium enterprises in Nairobi County.
ii. To find out the influence of information technology awareness and training on the performance of small and medium enterprises in Nairobi County

iii. To determine how system monitoring and maintenance influences the performance of small and medium enterprises in Nairobi County

iv. To establish the influence of access control on the performance of small and medium enterprises in Nairobi County

1.4 Research Questions

This study sought to answer the following research questions;

i. How do information technology policies influence the performance of small and medium enterprises in Nairobi County?

ii. How does information technology awareness and training influence the performance of small and medium enterprises in Nairobi County?

iii. How does system monitoring and maintenance influence the performance of small and medium enterprises in Nairobi County?

iv. How does access control influence the performance of small and medium enterprises in Nairobi County?

1.5 Significance of the Study

This study's findings are of benefit to a number of stakeholders in the information technology and small and medium enterprises. The study may benefit the management of SMEs in Nairobi County as it provides information on how various information technology security practices influence the performance of their businesses. The study also provides information on how these information technology security practices can be used to improve performance.

SMEs are important pillars of Kenya's economy. Therefore, to the GoK and policy makers; the study provides important information that is essential in making policies that enhance technology security among small and medium enterprises in an effort to improve their performance. The study provides information that can be used in formulating policies to shelter other stakeholders like consumers.

The study improves other researchers' knowledge pertaining information technology security practices and performance of SMEs. The study also offers a platform for other researches on various information technology security practices used by small and medium enterprises and how they influence their performance.

1.6 Scope of the Study

This study only focused on 1,221 SMEs in the hotel sector in Nairobi County. In addition, the study targeted the owners or the managers of the SMEs. SMEs are considered to be businesses that employ between 5 and 50 employees. The sample size of this study was 292 SME owners or managers. This process was undertaken over a period of one month.

1.7 Limitations of the Study

Some of the owners and the managers of SMEs in Nairobi County were reluctant to give permission to proceed with the research as performance of SMEs as well as information technology security practices are matters considered confidential to their businesses. The researcher however notified the management that the study is solely for academic purposes. The researcher also obtained a data collection letter from Kenyatta University.

1.8 Organization of the Study

The research project comprised of three chapters. Chapter one is the introduction and consists of the background of the study, statement of the problem, objectives of the study which has the general objective and the specific objectives, research questions, significance of the study, scope of the study, assumptions of the study, and limitation of the study. Chapter two is the literature review and shall comprise of a theoretical review, empirical review and the summary of the literature and research gaps. The chapter also presented the conceptual framework. Chapter three focused on the research design, target population, sampling design, data collection instruments, data collecting procedures and lastly data analysis and presentation. Chapter four presented the analysis of data and interpretation of the findings. Chapter five presented discussions of the findings, conclusions drawn from the findings, recommendation and suggestions for further studies.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Reviews of literature on effects of information technology security practices on SMEs performance are presented in this chapter. It starts off with a theoretical review then the empirical review, a summary of review of literature and the conceptual framework.

2.2 Theoretical Review

The section reviews relevant theories and models that support the effects of information security practices on SMEs within Nairobi County. The theories are systems theory and the general deterrence theory.

2.2.1 Systems Theory

Systems theory dates back to the 1940s when Bertalanffy began to connect systems theory with wholeness. According to systems theory, a system essentially consists of objects (physical or logical), attributes that describe the objects, relationships among the objects and the environment in which the system is contained. Systems theory treats organizations as open systems. Open systems are systems that are affected by the environment (Bertalanffy, 1968).

Systems theory is a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unforeseen ways. Studying the behaviors and results of the interactions can assist the management of an organization to better understand the organizational system and the way it functions (ISACA, 2009)

A system may show characteristics that are not related to individual system characters. These are known as emergent properties. Security, a frequent emergent property in a system, is not directly pegged to a specific component but is caused by the interaction of a number of components as they try to attain the desired result (Alter, 2015). Failure of enterprises to adequately address security issues in recent years is due to their inability to define security and present it in a way that is logical and relevant to all stakeholders (ISACA, 2009)

Designing security solutions for today's computer systems is a challenge. The modern business environment is made up of many different applications such as e-mails, databases, e-commerce, and more. Each of these applications has its own threat profile and associated business risk that must be taken into account (ISACA, 2009)

Current methodologies for designing security systems include piecemeal designs and patchwork systems comprised of multiple point solutions. As the complexity of the business driven systems increase, these methods are being strained to keep up with security requirements. Analysis and design of security systems using systems theory provides a new path to reduce the complexity (ISACA, 2009)

2.2.2 General Deterrence Theory

The general deterrence theory can be traced to the early works of classical philosophers such as Thomas Hobbes, Cesare Beccar, and Jeremy Bentham. It is one of the most widely applied theories in information systems (IS) security research, particularly within behavioral IS security studies. According to the theory, wrongful activities can be controlled by the threat of sanctions that are certain, severe, and swift (Darcy and Hearth, 2011)

Darcy and Hearth (2011) define counter measures as collection of organizational devices that are used to prevent or point out a security breach. This enhances the appropriateness of GDT due to its dimensions; detection, prevention, remedy and deterrence. It is an origin of criminology and some of its early work includes examining deterrence, detection, prevention and using remedies to influence crime rates. It mitigation can be used to reduced risk by use of deterrence remedy and detection techniques.

Quackenbush (2010) the aim of security efforts is to prevent the occurrence of computer abuse. Majority of organizations do not take systematic approaches to detect abuse of computers. Johnson, Leeds and Wu (2015) agreed that purposeful detection requires understanding the role of detection activities to identify breaches. They also noted that computer abuse detection is noted through normal system use as opposed to accidental or purposeful investigation.

Lijiao (2014) remedy efforts were explored in terms of internal and external sanctions. Internal remedy is applicable to business partners or colleagues. An external remedy on the other hand includes issues such as filing of police reports, indictment, prosecution and conviction. They serve as recourse against outsiders in an organization. The main aim of deterrent efforts is to offer disincentives for probable computer abusers so as to prevent them from abusing computers. This can be done through employee training, administrative policies and visible security functions (Lijiao (2014).

Kankanhalli (2003) realized that the use of preventive efforts leads to a more efficient Information Systems Security effectiveness, although they can also affect functioning of a business and even lower a firm's profit. It then follows that prevention methods should be used

strategically to reduce the impact on a company's operations and at the same time offering protection to the firm.

The process of trying to point out breaches in security in an organization is known as detection. Lee, Lee and Yoo (2004) discovered the three methods of pointing out computer abuse which include purposeful detection activities, accidental discovery and discovery through internal systems controls.

2.3 Empirical Review

2.3.1 Performance of Small and Medium Enterprises

As Taylor and Taylor (2014) highlight, effectiveness relates to how the demands of the various interested parties in a firm have been reached while efficiency relates to the way that a firm's assets are used in production with little or no wastage to the resources availed. To gain a competitive advantage, every firm has to make its future results attainable through greater satisfaction of the stakeholders and minimal wastage of resources compared to their competitors (Shin, 2015).

According to Tomsic, Bojnec and Simcic (2015), performance is specifically comprised of three major fields of the organization results, which include the use of the assets to generate revenues, (profits, return on assets, return on investment, etc.); the amount of output (sales, market share); and gains of the investor from the investment (total shareholder return, economic value added). According to Mutandwa, Taremwa & Tubanambazi (2015), a business organization ought to measure its performance using both financial and non-financial standards.

The degree in which a firm can use its resources from the basics to generate revenue can be reviewed from her accounts e.g. the company's summary of the revenues, costs and expenditure

or the balance sheet. In any organization, an individual staff's degree of utilizing the organization's resources to generate revenue should be measured and verified. Apart from the objective measures that can be quantified and verified (financial measures), there is need to include measures of performance that are not financially oriented also known as the subjective measures of performance, so as to have a rounded measurement of performance. (Taylor & Taylor, 2014).

In this study the financial oriented indicators such as Return On Assets (ROA), sales growth, Return On Equity (ROE) and profitability growth together with non-financial factors such as employee growth, satisfaction with execution compared to other similar businesses customer satisfaction and overall satisfaction was used to assess the SMEs.

2.3.2 Information Technology Policies and Performance of SMEs

A policy gives explanations on matters like threats and it details what should one do in case one occurs. Procedures and mechanisms of safeguarding of the company's information should also included in the policy (Sharma, Bhagwat & Dangayach, 2008).

In a research carried out by Kimwele, Mwangi and Kimani (2011), in which the objective was to determine the extent that Kenyan small and medium Enterprises have gone towards adopting the Information Technology Security Policies, it was discovered that the enterprises are still not taking this aspect as important with some of them disregarding the need for IT policies. How the duties and the responsibilities of Information Technology (IT) in the SMEs has been defined; if there is a documentation of the information security; and if the employees are aware of the policy, are some of the things covered in the study. In order to establish the acceptability of information security policies, factors that need to be considered are, the time when the SME

started; the duration within which the firm has been using computers; awareness and sensitization level of the employees on the application of the information systems; as well as the level at which the SME offers reliable and proper security training. The study also established that information security policies are important in attaining a continuous method for improving the organization's information security (Kimwele, Mwangi and Kimani, 2011)

The main of Information Technology policies is controlling the accessibility of information where the rules and regulations of the company apply in the control. It also ensures the reliability and the authenticity of the information gotten from the company. The policy makes sure that the information can be easily accessed by the people who are authorized to access it when they need it. In an aim of determining the impact of information system security policies and controls on firm operation enhancement for Kenyan Small and Medium Enterprises, Ogalo (2012) conducted a study in Kisumu central business district where he surveyed a targeted population of 481 SMEs in Kisumu. In his findings, he discovered the need for organizations to create strategies that give importance to ICT infrastructure investment and management. After formulating the strategies there follows the establishment of directions on putting into action and controlling them. In addition, regular checkups are important for early detection of any problem that may arise and adversely affect the ICT programs (Ogalo, 2012)

Finally, the government of Kenya has a responsibility to encourage and improve the use of ICT by making sure that the policies are binding and supportive. This can be done by creating information policies that will help the SMEs country wide as well as provide the required training on how to use ICT. Collaboration and partnerships can be fostered with other technologically advanced economies for purposes of sharing information needs and business requirements (Ogalo & Nyangara, 2011).

2.3.3 Information Technology Awareness and Training and Performance of SMEs

The impact of Information Technology systems is seen through the involvement of people with information technology. Behavior is having people behave in a particular way and this is what information security is mainly made up of according to Tidwell (2013). The need for security tools has increased over the years and ICT specialists have tried to automate very many security processes but some are not yet automated and others may not be automated. Technologies to provide security sorely depend on the way they are implemented and operated by human beings. Therefore, the people in an organization determine the degree of security of the company. Adequate training is required for people as they deal with ICT systems as they appear to be most unreliable link in information security (Dinev & Qing, 2007).

Darcy, Hovav and Galletta (2008) conducted a study on the knowledge of a user when dealing with a security threat and the effect it has on the misuse of information systems. The study presented criminology, social psychology and information systems combined in one theory model. From the model, it was assumed that sensitization of a user of security threats has direct effect on the perceived confidence and the threats of organizational sanctions associated with IS misuse, which leads to reduced IS misuse intention. The model was piloted on 269 computer users from eight different companies. The results from the excercise revealed that three practices discourage IS misuse: user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring.

Dinev and Qing (2007), argue that in order to make security processes effective there is need to properly understand their requirements and support. For example, an employee needs to know and understand a security incident and how to act if the incident occurs. If this knowledge is not imparted, it makes a well-crafted incident management process useless. Security awareness in

this situation becomes completely unreliable. Practitioners have the responsibility to link the knowledge of the user and the correct behavior needed from them. Education should be on what is supposed to be done as well as why it is being done. They users will then be able to at least reduce the impact of any threat that appears. Beachboard , (2008)

2.3.4 System Monitoring and Maintenance and Performance of SMEs

The foundation of proper handling of information systems is continuously checking the function ability of the key areas (Vijayakumar & Ilangovan, 2015). It appears to be very boring and un creative job and most specialists in IT have no time for but it is very important. Skipping of regular check- ups can result to break down of the systems, time wastage and data loss. Beachboard, (2008). Attending to the information systems from time to time can save the organization from occurrences that can negatively impact on it if they happen. Keeping a timetable of the maintenance of the information systems is an important factor in keeping the entire system healthy. Regular monitoring and preventive measures of systems is very crucial so as to assure smooth operation of the IT systems (Yeniman , 2011).

Periodically checking the information systems for deficiencies through control points is what monitoring and preventative maintenance service includes (period of diagnosis depends on customer requirements) (Vijayakumar & Ilangovan, 2015). The periodic checking may consist of automatic observation of key indicators of the state of the information systems; regular procedural maintenance of equipment in the field within a given schedule; and detailed report on the state of the system. Monitoring and preventative maintenance service also comprises of immediate reporting to the customer's specialists in case of divergence from the normal system operation (Cholez & Girard, 2014).

A combination of routine check up and the series of changes in the system development cycle is required to establish if the security controls in the information system continue to be reliable even after the unavoidable changes that are done to the system as well as in the environment in which it operates (Vijayakumar & Ilangovan, 2015). A Security Life Cycle defines the requirements for a continuous monitoring process. A routine monitoring program enables an organization to follow the security condition of an information system on a regular basis; and maintain the security authorization for the system. As changes occur in an information system and its environs, it is the duty of the information owner to make sure that the system authorization remains current, and updates the critical security documents (Cholez & Girard, 2014).

2.3.5 Access Control and Performance of SMEs

Computer security involves ensuring that the data in a system is unavailable to people who are unauthorized to get into contact with it and protecting the computer from destruction. System users, security practitioners, administrative personnel and system operations personnel aim at striking a balance between security and productivity because some security controls slow down productivity (Rui-Feng, Ning & Yu, 2012).

Administrative controls, technical controls or physical controls are some of the access controls that enhance information security. A further classification of these categories is either preventive or detective access controls. Preventive controls try to mitigate any risks that may occur, while detective controls identify unwanted events following their occurrence (Fotiou, Marias & Polyzos, 2012).

Preventive controls decrease free usage of computing resources and hence can only be used to a degree acceptable to the users. Effective training on security programs is therefore needed as it helps in improving the level of tolerance among the users as they are able to understand the importance of such controls in making it possible for them to trust their computing systems (Upfold & Sewry, 2008). Examples of preventive controls include access control software, antivirus software, encryption, library control systems, smart cards, passwords, callback systems and dial-up access control and (Cholez & Girard, 2014). Preventive technical controls hinder unauthorized people or programs from getting reach to the computing resources. This is done using safeguards integrated in the tangible and intangible computer components, operations or applications software, communication hardware and software together with other related components. Detective controls tools include intrusion detection methods, audit trails and checksums.

Physical security is controlling the access to computers, related materials and objects (including utilities) and the processing facility itself by use of locks, alarms, security guards, badges, and other related measures. More so, mechanisms to secure computers from destruction from either fire, water, natural disaster including floods and earthquakes, or physical theft by people and its related equipments and contents from espionage are a requirement (Vijayakumar & Ilangovan, 2015). Biometric access, file backups, and security guards are examples of physical measures applicable in controlling who enters the areas with computers and related equipments.

In providing an adequate level of protection for computing resources, the administrative controls used include operational procedures, accountability procedures, management constraints, and supplemental administrative controls (Yeniman, 2011). Administrative controls consists of

mechanisms designed to make sure that proper authorizations and security clearances are given to the people allowed to access the computing resources. Examples of preventive administrative controls include separation of duties, procedures for hiring and firing personnel, registration of people who are authorized to get access to computers, security policies and guidelines as well as supervision, disaster recovery, contingency, and emergency plans (Rui-Feng, Ning & Yu, 2012).

Upfold and Sewry (2008) found that only 52 percent of the respondents used custom user accounts and passwords in their firms in an investigation of Information Security in Small and Medium Enterprises in the Eastern Cape. This sends a red signal considering that user accounts and passwords are the only way of enforcing controlled access to resources. At start-ups, these enterprises have limited resources and mostly use unreliable systems mostly without proper regulations on the accessibility. With time the SMEs managers must restrict system access. There is therefore need to introduce a central unit of controlling users so as to ensure that the employees adhere to the basic security procedures e.g. individual accounts logons and passwords.

2.4 Summary of the Literature Review and Research Gap

This study used the systems theory and general deterrence theory to expound the effect of information technology security practices on the results of SMEs in Nairobi County. With regard to system theory, a system is complex and comprises of many components. Security is one of the emergent properties in systems. One of the requirements of security is strong defense - the use of various mechanisms to attain better standards of security. Lack of a proper approach in dealing with security issues hampers progress of SMEs. It therefore implies that SMEs should make use of several security practices at the same time in order to enhance security, noting that each information systems application has its own threat.

As applied to information technology security, the general deterrence theory suggests that threats can be mitigated through the use of deterrence, prevention, detection, and remedy techniques. This is because; wrongful activities can be controlled by the threat of sanctions.

The literature above shows that the process of risk mitigation associated with information security requires a detailed and standardized information security policy. Policies define issues such as information security threats and their countermeasures. They also define roles and responsibilities of all the employees in an organization in relation to information technology security. Information security policy specifies the systems, tools and procedures necessary in protecting information in an organization. The literature also shows that Information Technology systems are dependent on people and hence awareness and training are key in enhancing security. In addition, timely routine monitoring and maintenance of information systems is a key to health of the whole IT infrastructure.

2.6 Conceptual Framework

The relationship between the variables of the study is shown in a conceptual framework. The performance of the small and medium enterprises was the dependent variable while the information technology policies, information technology awareness and training, system monitoring and maintenance and access control were the independent variables. Figure 2.1 gives a representation of the conceptual framework reflecting the relationship between the various variables of the study.

Independent Variables **Dependent Variable**

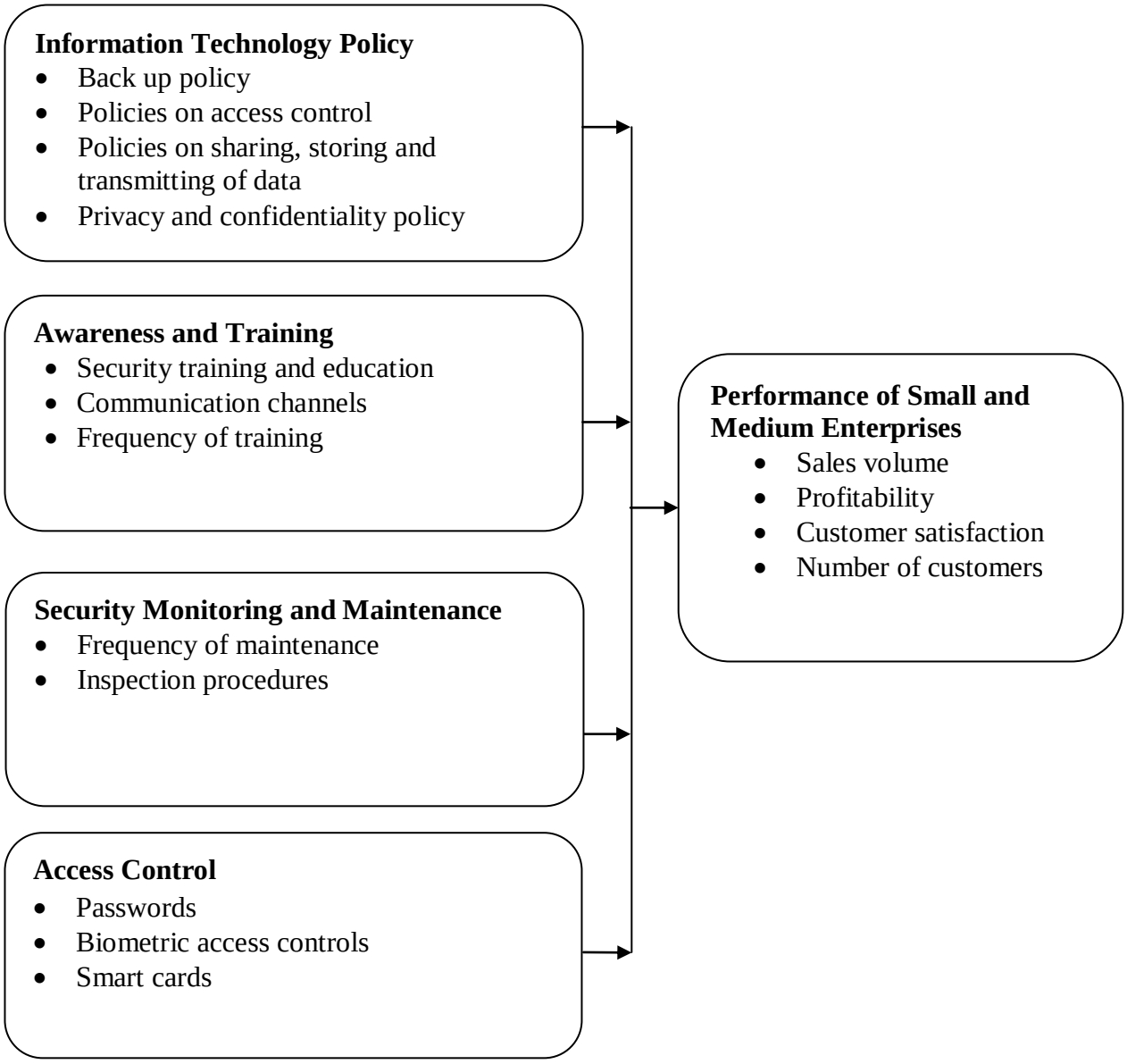

Figure 2.1: Conceptual Framework

Source: Author (2017)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research design, target population, sample size and sampling technique, data collection instruments, data collection procedure, pilot test and data analysis and presentation.

3.2 Research Design

This study used descriptive research design. Descriptive research design involves data collection, description of occurrences and thereafter organizes, depicts, tabulates and describes the data. According to Greener (2008), descriptive design is used to answer the research questions of the subject being studied after gathering the required data. The descriptive research design allows the researcher to make use of both the qualitative and quantitative data in gathering data and behaviors of the population or the event that the study is dedicated.

3.3 Target Population

The target population of this study was owners and managers of SMEs in the hotel sector operating in Nairobi County. Small and medium enterprises are businesses that employ between 5 and 50 employees. The SMEs dealing with the hotel sector in the records of Nairobi County government was 1,221 (Mochoge, 2014). The target population of this study was therefore 1,221 SMEs owners and managers in the hotel sector in Nairobi County.

3.4 Sampling and Sample Size

The study's sample size was determined by use of Krejcie and Morgan formula (Kothari, 2004). It is common practice for most studies for the confidence level to be at 95 percent and a precision +/- 5 percent. This was adopted in the study. The population for this study was 1,221. Therefore for the sample size at 95 percent confidence level, the following formula was applied.

$$n = \frac{X^2 * N * P * (1 - P)}{(ME^2 * (N - 1)) + (X^2 * P * (1 - P))}$$

Where;

N= sample size

X^2 = Chi-square for 95 percent confidence level at 1 degree of freedom

N=Population size

P= Population proportion

ME=Desired margin of error (expressed as a proportion)

$$= \frac{3.841 * 1221 * 0.5 * 0.5}{(0.05^2 * (1221 - 1)) + (3.841 * 0.5 * 0.5)}$$

n=292 SME owners or managers.

This study used simple random sampling technique to select 292 SME owners or managers from the target population. Simple random sampling was used in the selection of a group of subjects (sample) from the larger group (population) (Cooper &Schindler, 2006). Each individual was randomly picked from the population and they all had the same probability of inclusion in the sample. The sample size of this study was 292 respondents.

3.5 Data Collection Instruments

Self -administered questionnaires with unstructured and structured questions were used in the study in collecting primary data. The questionnaire explained the problem of the study together with its objectives and it contained both the open -ended questions and the closed ended questions. Only a particular type of response was required from the closed ended while the open- ended type, gave the respondents' the freedom to express their views. To be economical in terms of time, energy and finances, self-administered questionnaires were preferred in this study (Cooper & Schindler, 2006). The structured questions were utilized in order to save money and time and simplify the analysis as structured questions are usually in quantitative form. Unstructured questions were also used

3.6 Data Collection Procedures

The researcher obtained a research permit from the National Commission for Science, Technology and Innovation (NACOSTI). The administration of questionnaires was done by dropping the questionnaires to the targeted individuals and picking them later after they filled them. According to Ngechu (2004), the Drop-off and Pick-Up (DOPU) method is effective in ensuring high results in response rates. Also, the Drop-off and Pick-Up technique is effective in reducing potential non-response bias by increasing response rate. The time -frame for the researcher to collect data from the respondents was approximately a month. The respondents were required to complete questionnaire as honestly and as completely as possible. The researcher assured the respondents that their identities would be treated with high confidentiality. The completed questionnaires were collected once filled out.

3.6.1 Pilot Test

The questionnaires were randomly administered to 10 percent of the sample size who were not included in the main study. Pilot testing assisted in anticipating how the performance of the research instruments would be and identifying an easy way of administering them.

Testing of the questionnaire with a selected sample of SMEs in Nairobi County was a measure of ensuring the reliability of the research instrument. Cronbach's Alpha value ranges between 0 and 1 was used to apply an internal consistency technique. Coefficient of between 0.6 and 0.7 is a commonly accepted rule of thumb that indicates acceptable reliability. In addition, a Cronbach's Alpha of 0.8 or higher indicates good reliability (Mugenda & Mugenda, 2003). The data from the pilot test was not included in the actual study. In this study, Alpha value was 0.82

3.6.2 Validity

According to Orodho (2007) validity is determines the degree to which the information produced after analyzing the data collected, covers the problem under investigation or corresponds accurately to the real world. The study used two types of validity: content validity and face validity. A probability where the respondent may interpret a question wrongly or even fail to understand it is called face validity. According to Ngechu (2004), pre-testing is one of the main ways of increasing possibility of face validity and content validity. In this study, the content validity was improved by consulting experts in the field of study, specifically the supervisor. In addition, the research instrument's face validity was improved by conducting a pilot test and changing any ambiguous and unclear questions.

3.7 Data Analysis and Presentation

The questionnaires in this study generated both qualitative and quantitative data. Qualitative data from open ended questions was analysed by use of thematic content analysis. Quantitative data was analyzed by use of inferential and descriptive statistics using Statistical Package for Social Sciences (SPSS version 22). Descriptive statistics such as frequency, mean, percentages and standard deviation were used in this study. Further, multiple regression analysis was used to investigate the relationship between the dependent (performance of SMEs) and the independent variables (information technology policies, awareness and training, access control and system monitoring and maintenance). The regression model in this study was;

$$Y = \beta 0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

Whereby Y = Performance of SMEs

X_1 = Information technology policies

X_2 = Information technology awareness and training

X_3 = System monitoring and maintenance

X_4 = Access control

ε = Error Term

CHAPTER FOUR

RESEARCH FINDINGS AND DISCUSSIONS

4.1 Introduction

This chapter covers the analysis of both qualitative and quantitative data as well as the interpretation of the findings. The main objective of this study was to investigate the effect of information technology security practices on the performance of small and medium enterprises in Nairobi County. The study also sought to establish how information technology policies, information technology awareness and training, system monitoring and maintenance as well as access control influence the performance of SMEs in Nairobi County.

4.2 Response Rate

The study had a sample size of 292 SME owners in the hotel sector in Nairobi County. Out of 292 questionnaires given, 264 responses were obtained, which gave a rate of 90.41 percent. A 100 percent response rate was not achieved as some of the questionnaires had some inconsistent information and some were half way filled and thus could not be used in the study. Kothari (2004) indicates that a 50 percent or more response rate is sufficient and satisfactory for analysis, which shows that 90.41 percent was an acceptable basis for drawing conclusions.

4.3 Sample Characteristics

As part of the general information, the respondents were requested to specify their gender, age bracket, level of education and work experience.

4.3.1 Gender of the Respondents

The hotels' owners and managers were requested to specify their gender. The findings were as presented in Figure 4.1.

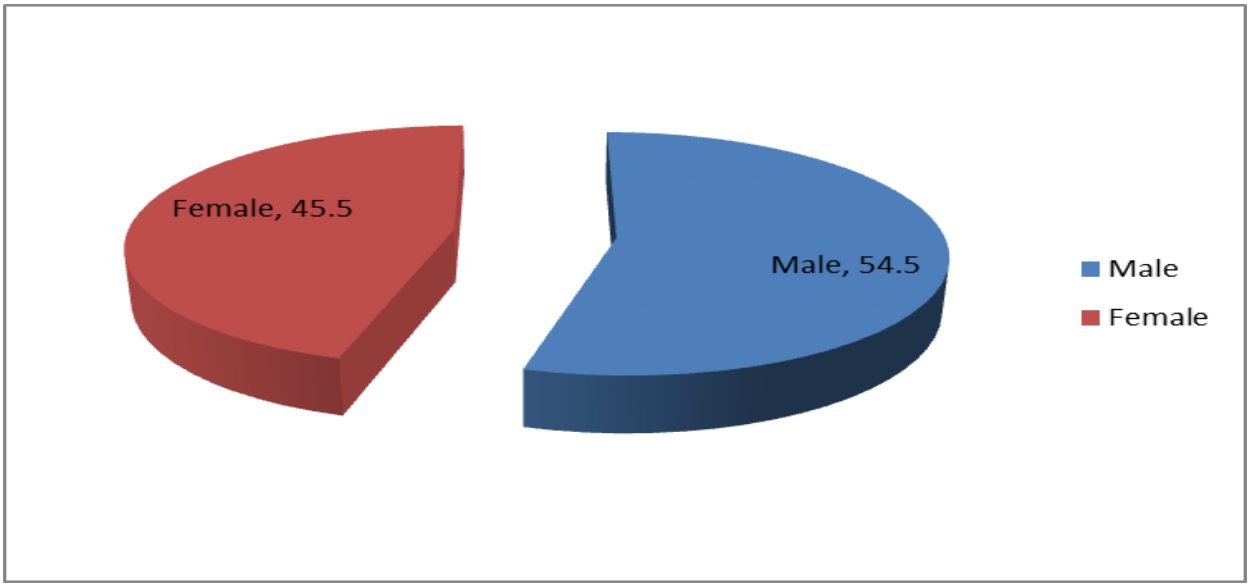

Figure 4. 1: Respondents' Gender

Source: Research Data (2016)

As indicated in Figure 4.1, 54.5 percent of the hotel owners and managers were male while 45.5 percent indiacted were female. This implies that the male hotel owners in Nairobi County were more than female hotel owners.

4.3.2 Respondents' Age Bracket

The hotel owners and managers were requested to specify their age bracket. The results were as shown in Figure 4.2.

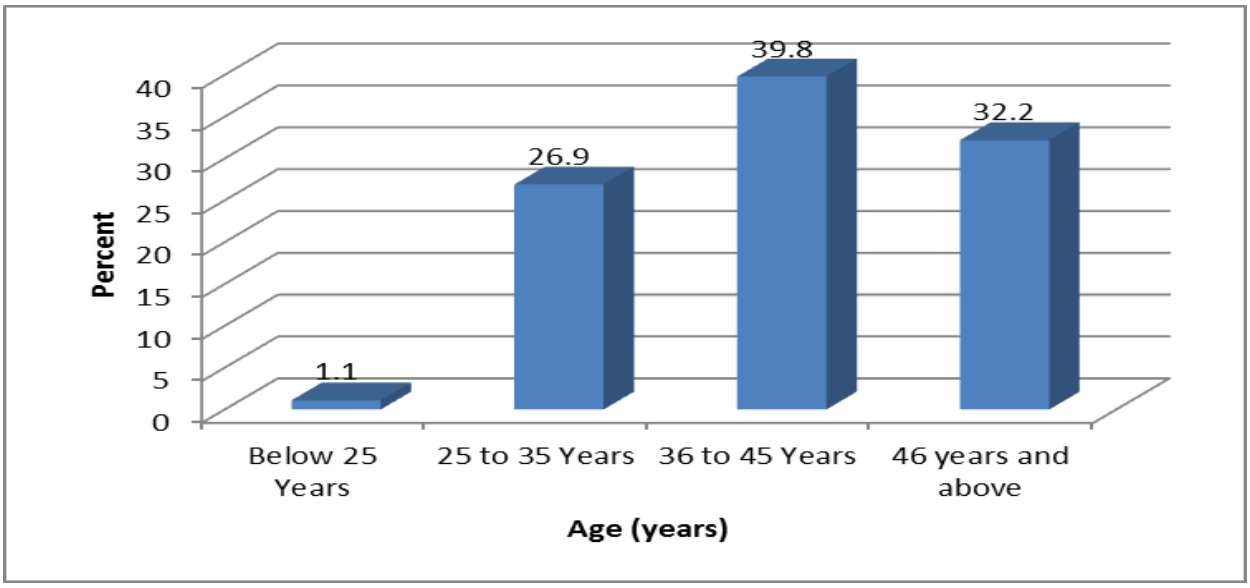

Figure 4. 2: Respondents' Age Bracket

Source: Research Data (2016)

As per Figure 4.2, 39.8 percent of the hotels' owners and managers were aged between 36 and 45 years, 32.2 percent were above 46 years of age, 26.9 percent indicated that their age was between 25 and 35 years and 1.1 percent were below 25 years of age. This implies that most of the hotel owners / general managers in Nairobi County were above 36 years of age.

4.3.3 Respondents' Highest Education Level

The hotel owners and managers were also asked to specify their level of education. The results were as presented in Figure 4.3.

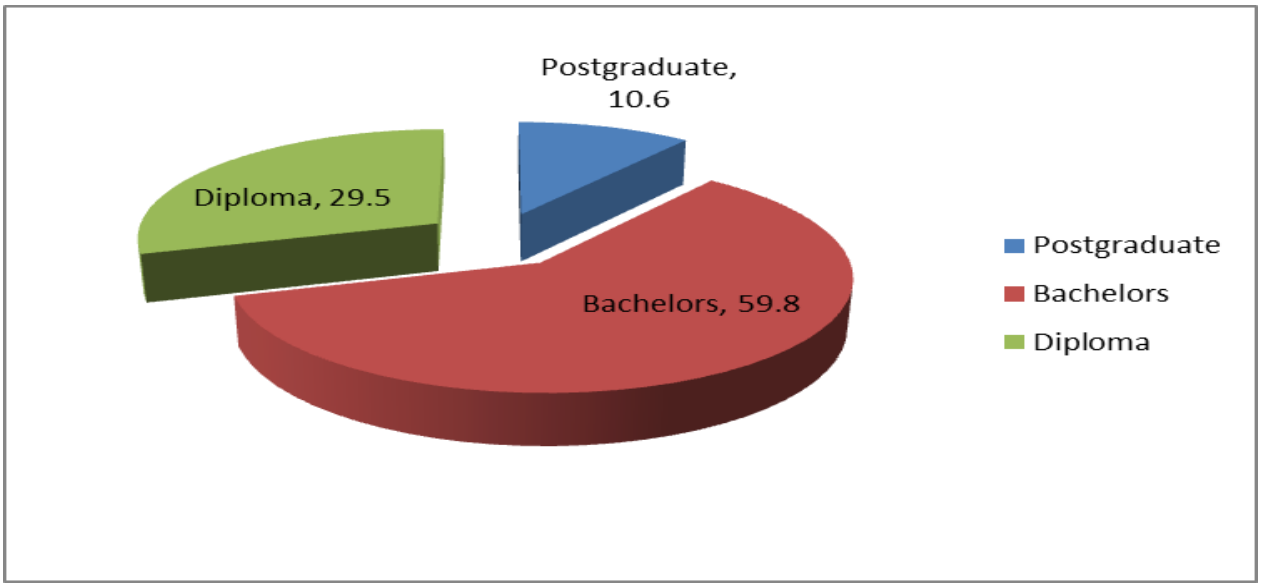

Figure 4. 3: Respondents' Highest level of Education

Source: Research Data (2016)

From the findings, 59.8 percent of the hotel owners and managers had bachelor's degree as their highest education level, 29.5 percent indicated that they had diplomas and 10.6 percent indicated that they had postgraduate degrees. This infers that most (59.8 percent) of the hotel owners and managers in this study had bachelor's degree as their highest education level.

4.3.4 Duration of Business Operation

The hotels' owners and managers were also queried on how long their businesses had been in operation. The findings were as shown in Figure 4.4.

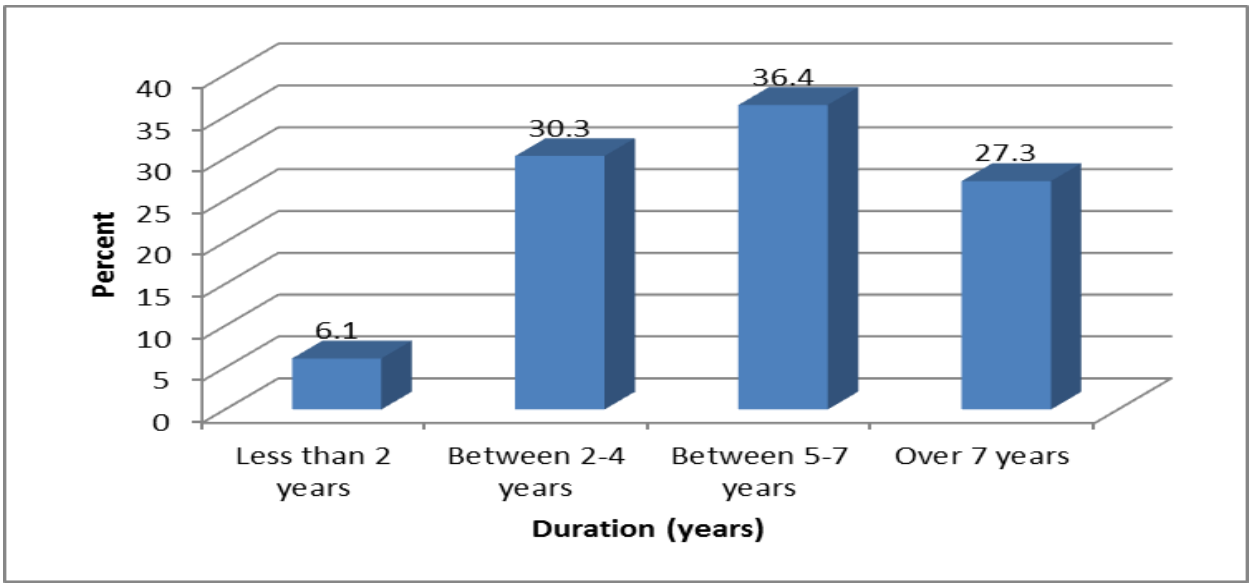

Figure 4. 4: Duration of Business Operation

Source: Research Data (2016)

According to the findings, 36.4 percent of the hotels' owners and managers reported that their business had been in operation for between 5 and 7 years, 30.3 percent indicated for between 2 and 4 years, 27.3 percent indicated for over 7 years and 6.1 percent indicated for less than 2 years. This shows that most of the hotels involved in this study had been in operation for more than 5 years and hence they had adopted information technology in their business operations.

4.4 Information Technology Policies

The first objective of the study was to establish how information technology policies influence performance of SMEs in Nairobi County.

4.4.1 Formal Information Technology Policies in Businesses

The hotels owners and managers were asked to indicate whether there were formal information technology policies in their businesses. The findings were as portrayed in Figure 4.5.

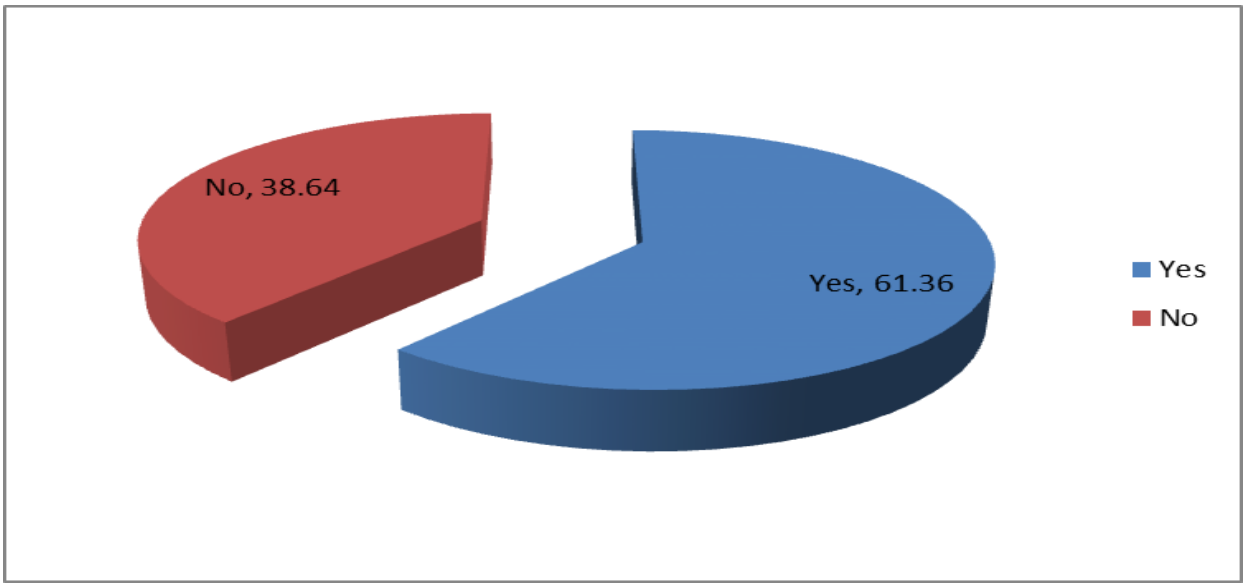

Figure 4. 5: Formal Information Technology Policies in Businesses

Source: Research Data (2016)

Research findings in Figure 4.5 indicate that 61.36 percent of the hotels owners and managers had formal information technology policies in their businesses while 38.64 percent disagreed. This suggests that most of the hotels in Nairobi County had formal information technology policies.

From the hotels' owners and managers who indicated that their businesses had formal information technology policies, the study in addition sought to determine the content of the information technology policy. They indicated that the content of the policy included encryption of sensitive information, encrypted wireless policy, back up p**o**licy, user access and privacy, password policy, consequences of misuse of ICT resources, database migration policy and system upgrade policy. The respondents also indicated that the policy had guidelines on acceptable access of the business systems. These findings agree with Sharma (2008) argument

that information security policy specifies the tools, system and procedures necessary in the protection of information in an organization.

4.4.2 IT Policies and Performance of SMEs

The hotels' owners and managers were asked to indicate the extent to which information technology policies influence the performance of SMEs in Kenya. The results were as shown in Table 4.1.

Table 4. 1: Influence of IT Policies on Performance of SMEs

	Frequency	**Percent**
No extent at all	1	.4
Moderate Extent	46	17.4
Great Extent	153	58.0
To a very Great Extent	64	24.2
Total	**264**	**100.0**
Average 66		

Source: Research Data (2016)

Table 4.1, 58 percent of the hotels' owners and managers reported that information technology policies greatly influence the performance of SMEs in Kenya, 24.2 percent indicated to a very great extent, 17.4 percent indicated to a moderate extent and 0.4 percent indicated to no extent at all. This shows that information technology policies influence the performance of SMEs in Kenya to a great extent. Despite its importance, Kimwele (2011) found that Kenyan SMEs appear to be lagging behind the development and utilization of IT security policy.

4.4.3 Aspects of Information Technology Policies

The hotels' owners and managers were further asked to indicate the extent to which various aspects of information technology policies influence the performance of SMEs in Kenya. A scale of 1 to 5 was used where 1 represents no extent at all, 2 represents low extent, 3 represents moderate extent, 4 represents great extent and 5 represents very great extent.

Table 4. 2: Aspects of Information Technology Policies

Aspects	Mean	Std. Deviation
Back up policy	3.704	1.111
Policies on access control	3.477	1.035
Policies on sharing, storing and transmitting of data	3.723	1.128
Privacy and Confidentiality policy	3.977	.849
Average	3.72	1.03

Source: Research Data (2016)

From the findings, the hotels' owners and managers indicated with a mean of 3.977 and a standard deviation of 0.849 that privacy and confidentiality policy influences the performance of SMEs in Kenya to a great extent. The hotels' owners and managers also indicated with a mean of 3.723 and a standard deviation of 1.128 that policies on storing, sharing as well as transmitting of data influences the performance of SMEs in Kenya to a great extent. These findings agree with Ogalo (2012) findings that policies regarding data access and management of information system have a significant effect on an organizations' performance. Further, the hotels' owners and managers indicated with a mean of 3.704 and a standard deviation of 1.111 that back up policy influences the performance of SMEs in Kenya to a great extent. The hotels' owners and

managers also indicated with a mean of 3.477 and a standard deviation of 1.035 that policies on access control influences his performance of SMEs in Kenya to a great extent.

4.4.4 Influence of IT policies on Performance of SMEs

The hotels' owners and managers were further asked to indicate how else information technology policies influence the performance of SMEs in Kenya. From the findings, the respondents indicated that information technology policies help in e-Marketing, access to business finance, e-commerce, like Business to Consumer and Business to Business and Business Branding. When perceived as secure a business can form collaboration with other businesses. In addition, the management can track efficiency and productivity of each member of staff and use this information to increase salary and wages and also award promotions. The management can mitigate risks like fraud caused by employees and outsiders. IT policies can also be used to define acceptable use of social media as a marketing strategy in order to give the business an edge over its competitors.

In addition, the hotels' owners and managers indicated that IT leads to increased company output from efficient processes, increased overhead cost from training, security measures and equipment, safekeeping of important information and cost reduction in accessing important information. However, the respondents also indicated that strict information technology policies are not widely adopted in the SMEs in Kenya due to lack of proper information and communication technology. These findings concur with Kimwele (2011) findings that IT security policy helps enterprises to maintain confidentiality of their information. In addition, it aims at creating limited access to enable the management of information in line with the protocols in the company.

4.5 Information Technology Awareness and Training

The second objective of the study was to find out the influence of information technology awareness and training on the performance of small and medium enterprises in Nairobi County.

4.5.1 Training on Information Technology Security

The hotels owners and managers were queried on whether they or any of their staff had received training on information technology security. The results were as shown in Figure 4.6.

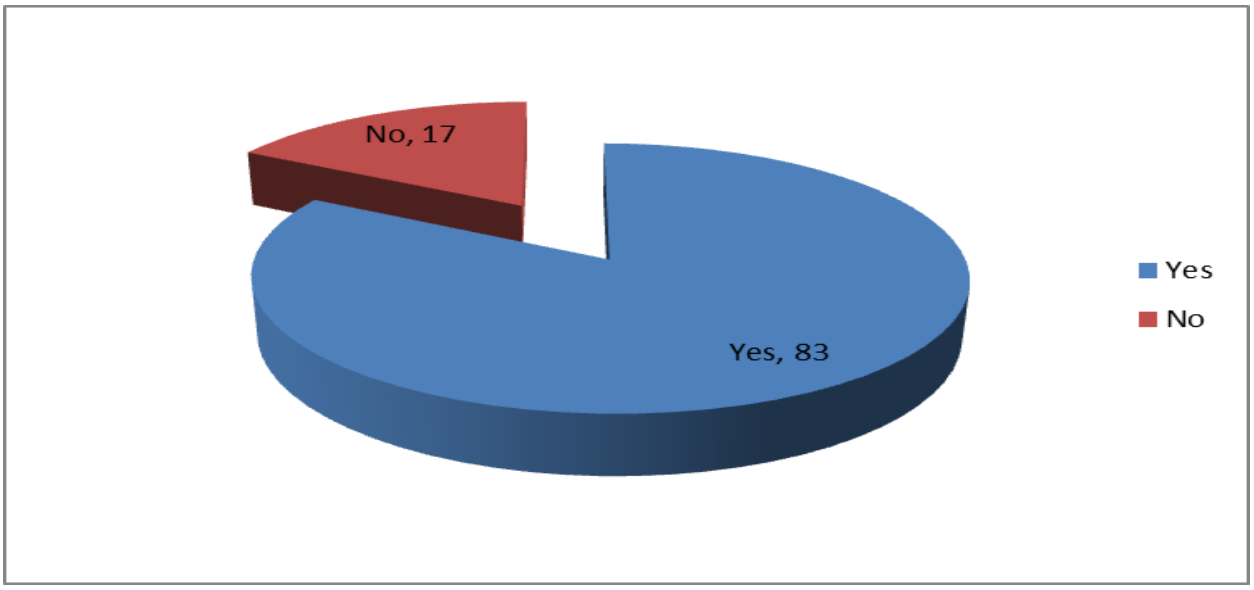

Figure 4. 6: Training on Information Technology Security

Source: Research Data (2016)

As per Figure 4.6, 83 percent of the hotels' owners and managers reported that their staff had received training on information technology security while 17 percent indicated that neither they nor their staff had obtained any training on information technology security. This implies that most of the owners as well as their staff had received some training on information technology

security. These findings concur with Dinev and Qing (2007) findings that IT security awareness and training influences organizational performance.

4.5.2 IT Awareness and Training and the Performance of SMEs

The hotels owners and managers were requested to show the extent to which awareness and training on information technology security influences the performance of SMEs in Kenya. The results were as shown in Figure 4.7.

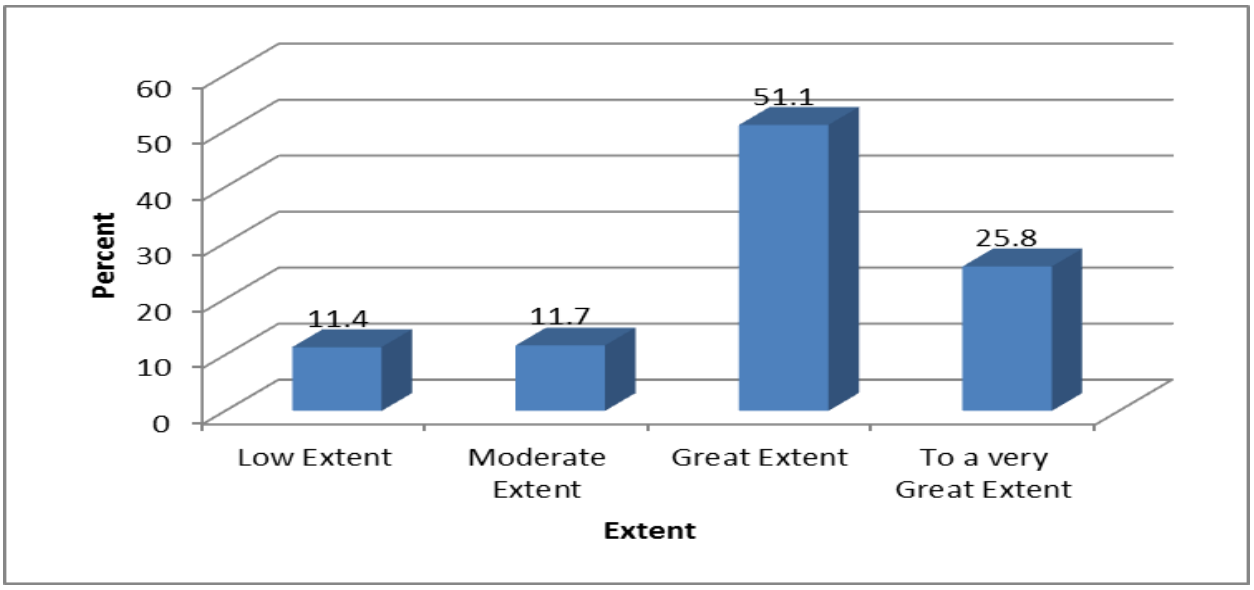

Figure 4. 7: IT Awareness and Training and the Performance of SMEs

Source: Research Data (2016)

As shown in Table 4.7, 51.1 percent of the hotels' owners and managers indicated that information technology awareness and training influences the performance of SMEs in Kenya to a great extent, 25.8 percent indicated to a very great extent, 11.7 percent indicated to a moderate extent and 11.4 percent indicated to a low extent. This implies that that information technology awareness and training influences the performance of SMEs in Kenya to a great extent. These

findings agree with Darcy (2008) who highlights the importance of training in enhancing information technology security, as it plays a major role in organizational performance.

4.5.3 Aspects of Information Technology Awareness and Training

The hotels' owners and managers were also requested to show the extent to which various components of information technology awareness and training influence the performance of SMEs in Kenya.

Table 4. 8: Aspects of Information Technology Awareness and Training

	Mean	Std. Deviation
Security training and education	4.075	.886
Communication channels	4.136	.684
Frequency of training	3.939	.900
Average	4.05	.0823

Source: Research Data (2016)

As indicated in Table 4.8, the hotels' owners and managers indicated with a mean of 4.136 and a standard deviation of 0.684 that communication channels influence the performance of SMEs in Kenya to a great extent. The hotels' owners and managers also indicated with a mean of 4.075 and a standard deviation of 0.886 that security training and education influences the performance of SMEs in Kenya to a great extent. This is in agreement with Beachboard (2008) argument that education and training is key in ensuring the information technology security of an organization. Further, the hotels' owners and managers indicated with a mean of 3.939 and a standard deviation of 0.900 that frequency of training influences the performance of SMEs in Kenya to a

great extent. These findings agree with Darcy (2008) that frequency of training plays a major role in enhancing information technology security and hence organizational performance.

4.5.4 Influence of IT Awareness and Training on the Performance of SMEs

The hotels' owners and managers were requested to indicate other ways in which information technology awareness and training influences the performance of SMEs in Kenya. From the findings, the respondents indicated that it makes it easy for them to collect, store and access the business data. Also, information technology awareness and training helps in computerizing operations and leads to increased awareness by capitalizing on the advantages of cyber advertising which could increase company productivity. Further, IT awareness and training is attractive to sophisticated personnel that tend to have a positive contribution to the diversity in skill level in the organization. In addition, it gives businesses a platform to exchange information on perceived threats in a particular industry and take steps to mitigate the risks. These findings are in line with Tidwell (2013) that training and awareness improves employee knowledge on various types of threats and ways of mitigating against them. It also provides a platform to engage with industry player and discuss on the most appropriate hardware and software to mitigate these risks.

4.6 System Monitoring and Maintenance

The third objective was to determine how system monitoring and maintenance influences the performance of SMEs in Nairobi County.

4.6.1 Monitoring and Maintaining Information Technology Systems

The hotels' owners and managers were asked to indicate whether their businesses monitor and maintain their information technology systems. The results were as shown in Figure 4.9.

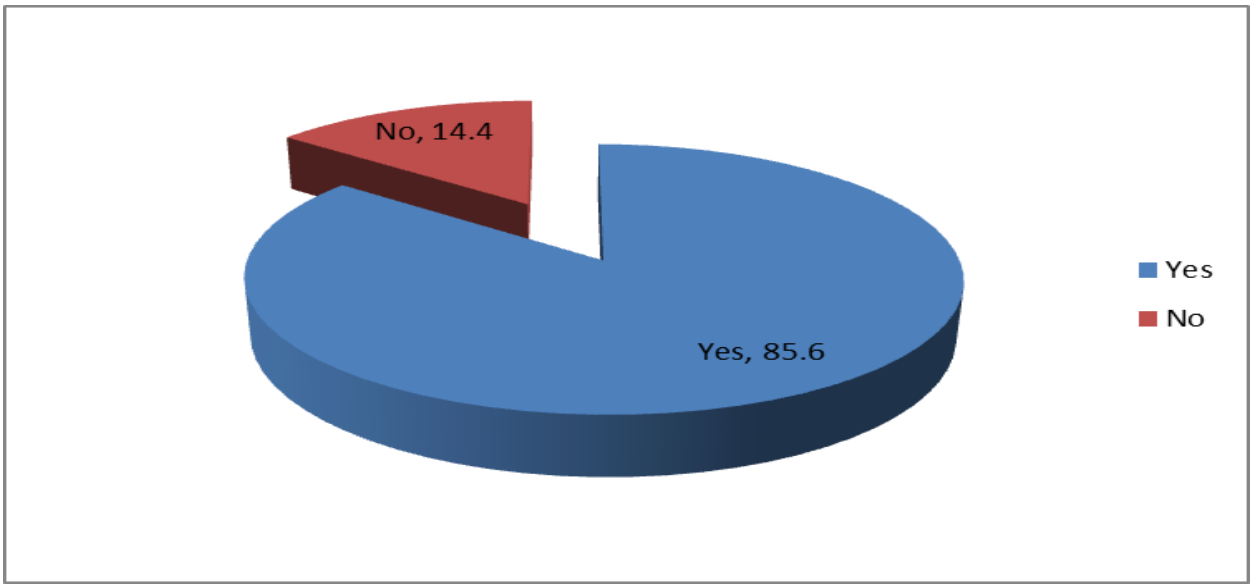

Figure 4. 9: Monitoring and Maintaining Information Technology Systems

Source: Research Data (2016)

As indicated above, 85.6 percent of the hotels' owners and managers indicated that their businesses monitor and maintain their information technology systems while 14.4 percent disagreed. This implies that most hotels in Nairobi County monitor and maintain their information technology systems. These findings concur with Ogalo (2012) findings that constant periodic assessment of information and communication technology risk is important in the identification of emerging threats that can have negative effects in information and communication technology assets utilization and operations.

4.6.2 Frequency of Monitoring and Maintaining Information Technology Systems

The hotels' owners and managers were further asked to indicate how often they monitor and maintain their information technology systems. The results were as shown in Table 4.3.

Table 4. 3: Frequency of Monitoring and Maintaining Information Technology Systems

	Frequency	Percent
Every week	72	31.9
Once in 1 year	49	21.7
Every 6 months	73	32.3
Once in 1 year	8	3.5
When there is a perceived threat	24	10.6
Total	**226**	**100.0**
Average 53.2		

Source: Research Data (2016)

As potrayed in Table 4.3, 32.3 percent of the hotels' owners and managers indicated that their businesses were monitoring and maintaining their information technology systems every six months, 31.9 percent indicated every week, 21.7 percent indicated once a year, 10.6 percent indicated when there is a perceived threat and 3.5 percent indicated once a year. This implies that majority of the hotels in Nairobi County were monitoring and maintaining their information technology systems every six months.

4.6.3 System Monitoring and Maintenance and the Performance of SMEs

The hotels' owners and managers were asked to specify the extent to which system monitoring and maintenance influence the performance of small and medium enterprises in Kenya. The results were as shown in Figure 4.10.

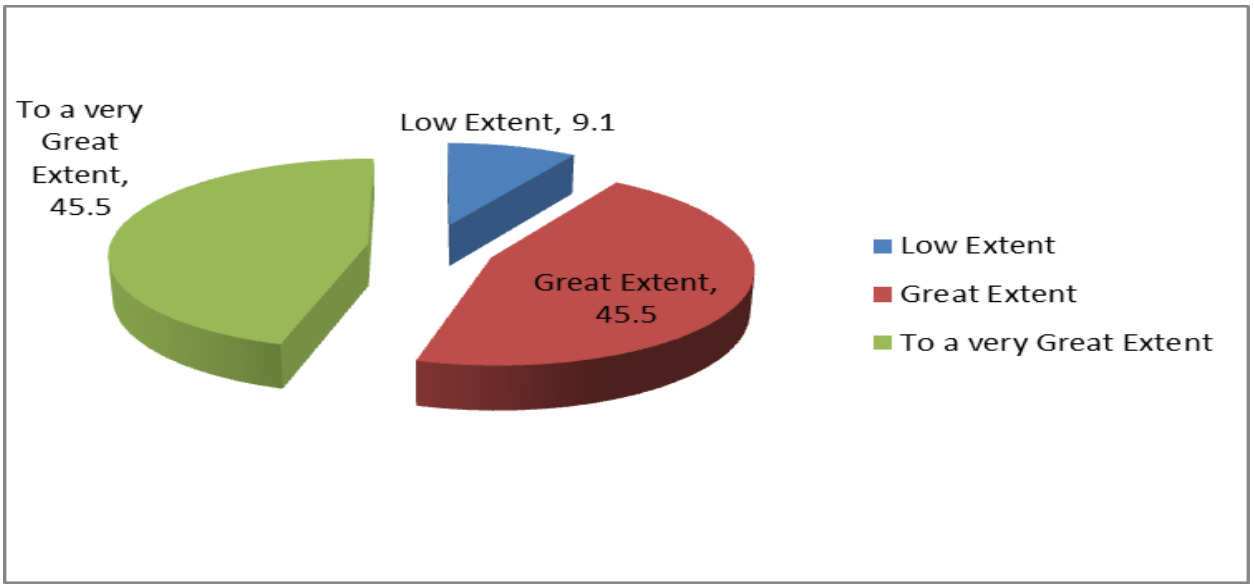

Figure 4. 10: System Monitoring and Maintenance and the Performance of SMEs

Source: Research Data (2016)

As shown in Figure 4.10, 45.5 percent of the hotels' owners and managers indicated that system monitoring and maintenance influences the performance of SMEs in Kenya to a great extent, the same percent indicated to a very great extent and 9.1 percent indicated to a low extent. These findings imply that system monitoring and maintenance influence the performance of SMEs in Kenya to a great extent. These findings are in line with Vijayakumar and Ilangovan (2015) argument that system monitoring and maintenance helps in identifying risks that can negatively affect the performance of a firm.

4.6.4 Aspects of System Monitoring and Maintenance

The hotels' owners and managers were queried on the extent to which various components of system monitoring and maintenance influence the performance of small and medium enterprises in Kenya. The results were as shown in Table 4.4.

Table 4. 4: Aspects of System Monitoring and Maintenance

	Mean	Std. Deviation
Frequency of maintenance	3.909	.884
Inspection procedures	3.848	.822
Average	3.87	.825

Source: Research Data (2016)

According to the findings, the hotels' owners and managers indicated with a mean of 3.909 and a standard deviation of 0.884 that frequency of maintenance influences the performance of SMEs in Kenya to a great extent. These findings concur with Yenima (2011) argument that timely information systems' routine maintenance is important in ensuring the health of the information technology infrastructure. The hotels' owners and managers also indicated with a mean of 3.848 and a standard deviation of 0.822 that inspection procedures influence the performance of SMEs in Kenya to a great extent.

4.6.5 Influence of Security Monitoring and Maintenance on the Performance of SMEs

The hotels' owners and managers were requested to indicate how else security monitoring and maintenance influences the performance of SMEs in Kenya. From the findings, the hotels' owners and managers indicated that security monitoring and maintenance ensures business information safety and any irregularities can be addressed immediately. In addition, by introducing controls and guidelines of information technology use, SMES are able to maintain data confidentiality hence a competitive edge. The hotels' owners and managers further indicated that with security monitoring and maintenance they do not have to worry about loss of sensitive

business related information which can negatively impact their businesses. Security awareness ensures that all users of information technology systems have a copy of the acceptable user policy and understand their responsibilities. These findings agree with Vijayakumar and Ilangovan (2015) argument that security monitoring and maintenance helps in tracking the security state of the system on a continuous basis and helps in maintaining the its security authorization.

4.7 Access Control

The fourth objective of the study was to establish the influence of access control on the performance of small and medium enterprises in Nairobi County.

4.7.1 Access Control Enhances Information Technology Security

The hotels' owners and managers were asked to specify whether they thought access control enhances information technology security. The results were as shown in Figure 4.11.

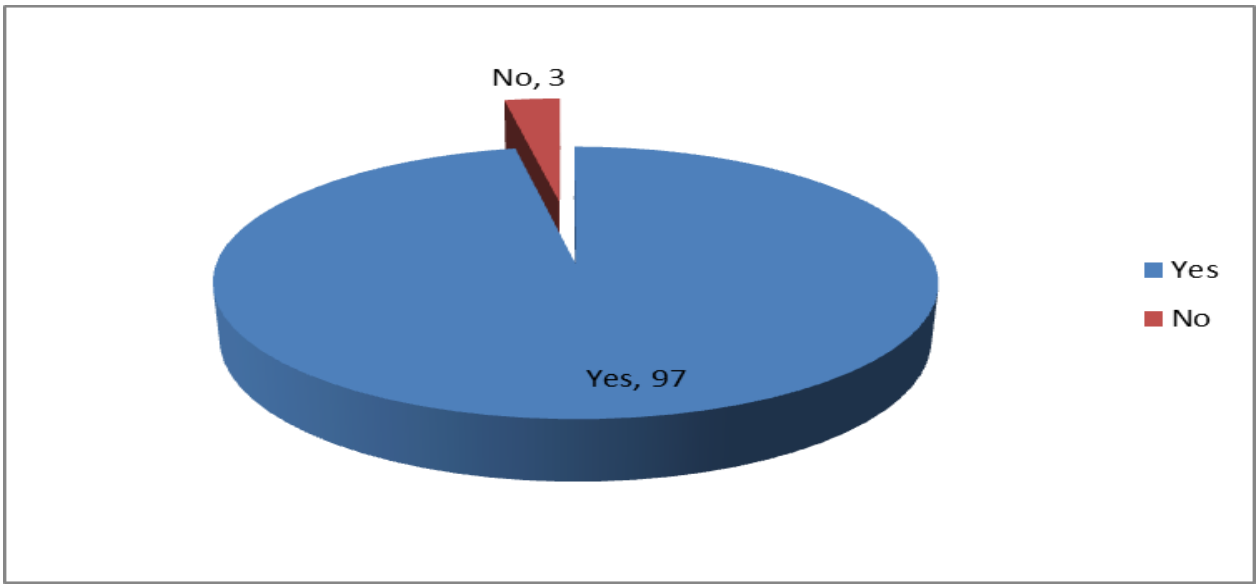

Figure 4. 11: Access Control Enhances Information Technology Security

Source: Research Data (2016)

Per the findings, 97 percent of the hotels' owners and managers indicated that access control enhances information technology security while 3 percent disagreed. This implies that access control enhances information technology security. These findings agree with Rui-Feng (2012) that access control is the cornerstone of security programs as indicated by most security professionals in information systems.

From the hotels' owners and managers who indicated that access control enhances information technology security, the study also sought to establish how. The hotels' owners and managers indicated that access control is considered as a security method, which is normally used in the regulation of who should view or access what in the computing environment. In addition, access control systems perform authorization identification, authentication and access approval. This is done through login credentials such as passwords, physical or electronic keys and biometric scans.

4.7.2 Access Control Measures Adopted to Enhance Information Technology Security

The respondents were also asked to indicate access control measures adopted to enhance information technology security in their businesses. The results were as presented in Table 4.5.

Table 4. 5: Access Control Measures Adopted to Enhance Information Technology Security

	Frequency		**Percent**	
	Yes	**No**	**Yes**	**No**
Use of passwords	244	20	92.4	7.6
Biometric access controls	124	140	47.0	53.0
Smart cards	160	104	60.6	39.4
Average	176	88	66.6	33.3

Source: Research Data (2016)

From the findings, 92.4 percent of the hotels' owners and managers indicated that their businesses had adopted use of passwords to enhance information technology security in their businesses, 47 percent indicated that they had adopted biometric access controls and 60.6 percent indicated that they had adopted smart cards. This shows that use of passwords was the most used access control measure to enhance information technology security in their businesses, followed by smart cards and biometric access controls.

4.7.3 Experience of Unauthorized Access in the last one year

The hotels' owners and managers were asked to indicate whether their businesses had experienced unauthorized access in the last one year. The results were as shown in Figure 4.12.

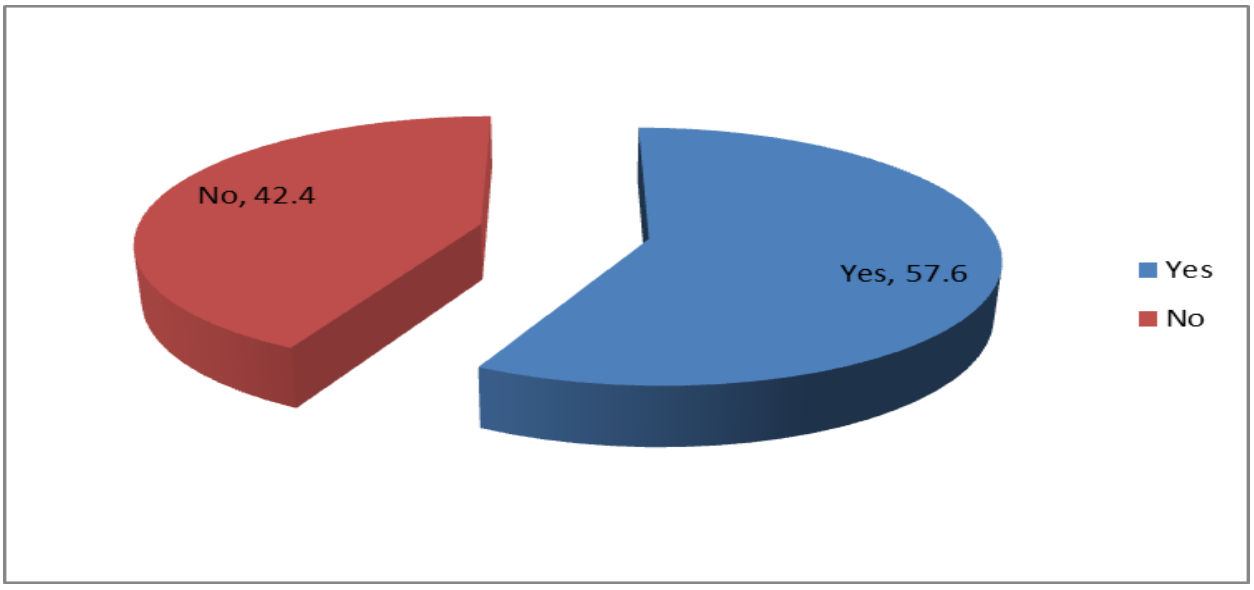

Figure 4. 12: Experience of Unauthorized Access in the last one year

Source: Research Data (2016)

From the findings, 57.6 percent of the hotels' owners and managers indicated that their businesses had experienced unauthorized access in the last one year while 42.4 percent disagreed. This implies that most of the businesses had experienced unauthorized access in the last one year.

4.7.4 Measures of Access Control

The hotels' owners and managers were queried on the extent to which various access control measures influence the performance of SMEs in Kenya. The results were as presented in Table 4.6.

Table 4. 6: Aspects of Access Control

	Mean	Std. Deviation
Passwords	4.030	.922
Biometric access controls	3.799	.800
Smart cards	3.674	.628
Average	3.834	.783

Source: Research Data (2016)

As indicated in Table 4.6, the hotels' owners and managers indicated with a mean of 4.030 and a standard deviation of 0.922 that passwords influence the performance of SMEs in Kenya to a great extent. The hotels' owners and managers also indicated with a mean of 3.799 and a standard deviation of 0.800 that biometric access controls influence the performance of SMEs in Kenya to a great extent. Further, the hotels' owners and managers indicated with a mean of 3.674 and a standard deviation of 0.628 that smart cards influence the performance of SMEs in Kenya

to a great extent. These findings correspond with Upfold and Sewry (2008) argument that the use of passwords, biometric access controls and smart cards influences the performance of SMEs.

4.7.5 Influence of Access Control on the Performance of SMEs

The hotels' managers and owners were requested to indicate how else access control influences the performance of SMEs in Kenya. They noted that it increases confidence to use the system, maintains the integrity of the system, safeguards the system and keeps off unauthorized persons. These findings agree with Yeniman (2011) argument that access control ensures that only authorized personnel should have access to computing resources, which enhances the availability, confidentiality and integrity of computing programs and data.

4.8 Performance of SMEs

The hotels' managers and owners were queried on the extent to which information technology security influences the performance of SMEs in Kenya. The results were as shown in Table 4.7.

Table 4. 7: Performance of SMEs

	Mean	**Std. Deviation**
Sales volume	3.825	.789
Profitability	3.935	.729
Customer satisfaction	4.200	.785
Number of customers	4.037	.817
Average	3.999	.78

Source: Research Data (2016)

As portrayed in Table 4.7, the hotels' managers and owners indicated with a mean of 4.200 and a standard deviation of 0.785 that information technology security influences customer satisfaction to a great extent. The hotels' owners and managers also indicated with a mean of 4.037 and a standard deviation of 0.817 that information technology security influences number of customers to a great extent. The respondents also indicated with a mean of 3.935 and a standard deviation of 0.729 information technology security influences profitability to a great extent. Also, the respondents agreed with a mean of 3.825 and a standard deviation of 0.789 that information technology security influences sales volume to a great extent.

4.9 Regression Analysis

The study used a multivariate regression analysis to determine the relationship between the dependent and the independent variables. The multivariate regression model was:

$$Y = \beta 0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

Whereby Y was Performance of SMEs, X_1 was Information technology policies, X_2 was Information technology awareness and training, X_3 was system monitoring and maintenance, X_4 was Access control and ε was the error term.

Table 4. 8: Regression Coefficients

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.219	.312		.702	.483
	Information technology policies	.435	.034	.597	12.706	.000

Information technology awareness and training	.299	.040	.343	7.471	.000
System monitoring and maintenance	.107	.041	.117	2.632	.009
Access control	.358	.060	.288	6.005	.000

a. Dependent Variable: Performance of SMEs

Source: Research Data (2016)

From Table 4.10, there is a positive significant relationship between information technology policies and the performance of SMEs with a regression coefficient of 0.435. This shows that a unit improvement in information technology policies would lead to a 0.435 improvement in the performance of SMEs. The p-value (0.00) was less than the significance level (0.05), hence the relationship was significant. These findings agree with Kimwele, Mwangi and Kimani (2011) findings that IT security policies positively influence organizational performance of SMEs.

The results also show that there is a positive significant relationship between information technology awareness and training and the performance of SMEs with a regression coefficient of 0.299. This shows that a unit improvement in information technology awareness and training would lead to a 0.299 improvement in the performance of SMEs. The relationship was significant as the p-value (0.000) was less than the significance level (0.05). These findings concur with Dinev and Qing (2007) findings that IT security awareness and training influences organizational performance.

From the findings, the study found that there is a positive relationship between systems monitoring and maintenance and the performance of SMEs with a regression coefficient of

0.107. This indicates that a unit improvement in systems monitoring and maintenance would lead to a 0.107 improvement in the performance of small and medium enterprises. The relationship was found to be significant as the p-value (0.001) was less than the significance level (0.05). These findings concur with Ogalo (2012) findings that systems monitoring and maintenance and the performance of SMEs.

Lastly, the study results show that there is a positive significant relationship between access control and the performance of small and enterprises with a regression coefficient of 0.358. This indicates that a unit improvement in access control would lead to a 0.358 improvement in the performance of SMEs. This relationship was significant as the p-value (0.005) was less that of the significance level (0.05). These findings concur with Rui-Feng (2012) findings that access control significantly influences the performance of SMEs.

Table 4. 9: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.730[a]	.533	.526	.42626

a. Predictors: (Constant), Access control , System monitoring and maintenance, Information technology awareness and training , Information technology policies

Source: Research Data (2016)

The R-Squared is the variation in the dependent variable which can be explained by the independent variables. From the findings, the R-squared in this study was 0.526, which shows that the four independent variables (information technology policies, information technology awareness and training, system monitoring and maintenance as well as access control) can explain 53.3 percent of the variation in the dependent variable. This clearly shows that other

factors not considered in this study explain 46.7 percent of the variation in the dependent variable, performance of SMEs.

Table 4. 10: Analysis of Variance

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	53.690	4	13.422	73.871	.000[b]
	Residual	47.060	259	.182		
	Total	100.750	263			

a. Dependent Variable: Performance of SMEs
b. Predictors: (Constant), Access control , System monitoring and maintenance, Information technology awareness and training , Information technology policies

Source: Research Data (2016)

From Table 4.10, the analysis of variance in this study was used to determine whether the model is a good fit for the data. The results indicate that the model was significant since the p-value (0.000) was less than 0.05 thus the model is statistically significance in establishing the influence of information technology policies, information technology awareness and training, system monitoring and maintenance as well as access control on the performance of SMEs. Further, the F-calculated (73.871) was found to be more than the F-critical (2.46) which shows that the models was fit in establishing the influence of the four independent variables on the dependent variable.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a discussion of the findings, conclusions drawn from the findings, recommendation and suggestions for further studies. The conclusions and recommendations were aimed at addressing the general objective of the study, which was to investigate the effect of information technology security practices on the performance of SMEs in Nairobi County.

5.2 Summary

SMEs play a major role in the economies of developing countries. In Kenya, in spite of having small and medium enterprises starting on a very high note, there is a high rate of collapse and most enterprises live for a short period of time. SMEs are ranked highest in regard to risk exposure related to information security. This high exposure to risk for SMEs leads to poor performance and high collapse rates. The study also sought to establish how information technology policies, information technology awareness and training, system monitoring and access control affect the performance of SMEs in Nairobi County. This research study used a descriptive research design. The target population was the 1221 owners or general managers of all the SMEs in the hotel sector operating in Nairobi County. The study adopted a simple random sampling method to select a sample size of 292 SME owners or managers from the target population. The study used primary data, which was collected by use of self-administered questionnaires. Qualitative data from open ended questions was analysed by use of thematic content analysis. The quantitative data was analyzed by use of descriptive and inferential

statistics. To examine the relationship between dependent and the independent variables a multiple regression analysis was used.

5.2.1 Information Technology Policies

The study found that most of the hotels in Nairobi County had formal information technology policies. The content of the policies included encryption of sensitive information, encrypted wireless policy, back up policy, user access and privacy, password policy, consequences of misuse of ICT resources, database migration policy and system upgrade policy. The study also established that information technology policies influence the performance of SMEs in Kenya to a great extent. The study revealed that a privacy and confidentiality policy influences the performance of SMEs in Kenya to a great extent. The study also found that policies on sharing, storing and transmitting of data influence the performance of SMEs in Kenya to a great extent. Further, the study established that back up policy and policies on access control influence the performance of SMEs in Kenya to a great extent.

The study revealed that information technology policies help in e-marketing, access to business finance, e-commerce and business branding since when perceived as secure a business can form collaboration with other businesses. In addition, the management can track efficiency and productivity of each member of staff and use this information to increase salary and wages and also award promotions. The management can also mitigate risks like fraud caused by employees and outsiders. IT policies can also be used to define acceptable use of social media as a marketing strategy in order to give the business an edge over its competitors. However, the respondents also indicated that strict information technology policies are not widely adopted in the SMEs in Kenya due to lack of proper information and communication technology infrastructure.

5.2.2 Information Technology Awareness and Training

The study established that most of the hotel owners, managers as well as their staff had received some training on information technology security. The study also found that information technology awareness and training influences the performance of SMEs in Kenya to a great extent. The study also further revealed that communication channels influence the performance of SMEs in Kenya to a great extent. The study also established that security training and education influences the performance of SMEs in Kenya to a great extent. Further, the study found that frequency of training influences the performance of SMEs in Kenya to a great extent.

The study established that information technology awareness and training makes it easy for staff and managers to collect, store and access the business data. Also, information technology awareness and training helps in computerizing operations and leads to increased awareness by capitalizing on the advantages of cyber advertising that could increase company productivity. Further, the study found that IT awareness and training is attractive to those seeking employment and thus the organizations are able to hire qualified personnel who are a positive contribution to the diversity in skill level in the organisation. In addition, it gives businesses a platform to exchange information on perceived threats in a particular industry and take steps to mitigate the risks.

5.2.3 System Monitoring and Maintenance

The study found that most hotels in Nairobi County monitor and maintain their information technology systems every six months.. The study also found that system monitoring and maintenance influences the performance of SMEs in Kenya to a great extent. The study established that frequency of maintenance influences the performance of SMEs in Kenya to a great extent. Timely information systems' routine maintenance of is important in ensuring the

health of the information technology infrastructure. The study also established that inspection procedures influence the performance of SMEs in Kenya to a great extent.

The study revealed that security monitoring and maintenance ensures the business information safety and any irregularities can be addressed immediately. In addition, by introducing controls and guidelines of information technology use, SMES are able to maintain data confidentiality hence a competitive edge. The study also found that with security monitoring and maintenance managers and owners of SMEs do not have to worry about loss of sensitive business related which can negatively impact their businesses.

5.2.4 Access Control

The study found that access control enhances information technology security. To most information systems security professionals, access control is the cornerstone of systems and programs' programs. The study also found that access control is a security measure that can be used to control who can view or use resources in a computing environment. The study revealed that use of passwords was the most used access control measure, followed by smart cards and biometric access controls. The study also revealed that most of the businesses had experienced unauthorized access in the last one year. The study established that the use of passwords, biometric access controls and smart cards influence the performance of SMEs in Kenya to a great extent.

The study established that access control increases confidence to use the system, maintains the integrity of the system, safeguards the system and keeps off unauthorized persons. In addition, SMEs are able to ensure that privacy and confidentiality is maintained.

5.3 Conclusion

This study concludes that there is a positive significant relationship between information technology policies and the performance of SMEs in Nairobi County. These findings agree with Kimwele, Mwangi and Kimani (2011) argument that information technology policies influence the performance of SMEs. The study found that privacy and confidentiality policy, back up policy as well as policies on sharing, storing and transmitting of data influence the performance of SMEs in Kenya. The content of an IT security policy should include encryption of sensitive information, back up policy, user access and privacy, password policy, consequences of misuse of ICT resources, database migration policy and system upgrade policy.

The study also concludes that there is a positive significant relationship between information technology awareness and training and the performance of SMEs in Nairobi County. These findings concur with Tidwell (2013) argument that information technology awareness and training influence the performance of SMEs. The study found that communication channels, security training and education as well as frequency of training influences the performance of SMEs in Kenya. Information technology awareness and training helps in computerizing operations and leads to increased awareness by capitalizing on the advantages such as cyber advertising could increase a company's productivity.

The study further concludes that there is a positive relationship between systems monitoring and maintenance and the performance of SMEs in Nairobi County. These findings are in line with Vijayakumar & Ilangovan (2015) argument that systems monitoring and maintenance influence the performance of SMEs. The study found that frequency of maintenance and inspection procedures influences the performance of SMEs in Kenya to a great extent. Routine maintenance

of information systems is key to health of the whole IT infrastructure. Monitoring and preventive maintenance of information systems service is therefore an important component in ensuring operability of company's IT systems

Lastly, the study concludes that there is a positive significant relationship between access control and the performance of SMEs in Nairobi County. These findings agree with Yeniman (2011) argument that access control influences the performance of SMEs. The study found that use of passwords was the most used access control measure to enhance information technology security, followed by smart cards and biometric access controls. The study also found that the use of passwords, biometric access controls and smart cards influence the performance of SMEs in Kenya.

5.4 Recommendations

From the findings in Chapter 4, the SME owners indicated that a significant investment by SMEs is required in order for ICT benefits to be realized. In addition, government support is required urgently by SMEs, in terms of funding, technology sharing and facilitation of SME collaboration with advanced ICT companies / countries. Also, the hotels' owners and managers indicated that a secure platform is re quired for SME to SME and SME to government technology integration. Further, the respondents indicated that ICT must be incorporated in the education system today for these are the SMEs of tomorrow. Policies, laws, rules and regulations must be fully implemented especially by regulators in order to protect SMEs and community at large. SMEs should upgrade their system, both hardware and software to keep up with the latest security features in the market. This could increase the efficiency in productivity while maintaining the integrity of data that could be compromised in case of a cyber-attack.

Despite the importance of IT security policy in guiding who should do what with information, the study found that more than one third of the SMEs had no IT security policy. This study therefore recommends that SMEs that have adopted information technology should come up with an IT security policy. The policy should comprise of use of passwords, encryption and consequences of misuse of ICT resources among others.

The study found that training awareness was key in ensuring information technology security. This study therefore suggests that the management of SMEs should plan for training programs on Information technology security. This will help in ensuring that the staff have up-to-date information on security risks and how to mitigate them.

The study found that most of the SMEs were conducting monitoring and maintenance of their information technology systems every six months. The study recommends that SMEs should consider increasing the frequency of monitoring and maintenance to once a month. This is because information technology risks are evolving and increasing every day as technology advances. In addition, SMEs should upgrade their system, both hardware and software to keep up with the latest security features in the market.

This study found that access control plays a major role in enhancing information technology security. The study therefore recommends that SMEs should make use of access control tools such as passwords, biometric access controls and smart cards to limit access. Constant periodic assessment of information and communication technology risk is important in the identification of emerging threats that can have negative effects in information and communication technology assets utilization and operations.

5.5 Suggestions for Further Studies

This study was limited to SMEs in the hotel industry in Nairobi County. SMEs in different industries utilize information technology differently and hence are exposed to different types of information technology security threats and risks. The study therefore suggests that further studies be conducted on effects of information technology security practices on the performance of all types of SMEs in Nairobi County. In addition, other aspects of information security such as collection of daily logs, monitoring of applications that access data and encryption of sensitive data should also be studied. The study also suggests further studies on Information technology security challenges facing SMEs in Kenya. The study further suggests further studies on the role of information technology in business operations in SMEs in Kenya.

REFERENCES

Alter, S. (2015). Work System Theory as a Platform: Response to a Research Perspective Article by Niederman and March. *Journal of the Association for Information Systems*, *16*(6), 485-514.

AusCERT (2005).*2005 Australian Computer Crime and Security Survey*, AusCERT.

Beachboard, J., Cole, A., Mellor, M., Hernandez, S. &Aytes, K. (2008). Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda.*Issues in Informing Science and Information Technology*, 5, 73-82.

Bertalanffy, L. (1968). *General System Theory: Foundations, Development, Applications*. New York: George Braziller.

Besnard, D. & Arief, B. (2004).Computer Security Impaired by Legitimate Users. *Computers & Security*, 23, 253-264.

Casaca, J.A. (2014). Determinants of the Information Security Effectiveness in Small and Medium Sized Enterprises. *The 3rd Electronic International Interdisciplinary Conference*, Lisboa, Portugal September, 1-5. 2014.

Caws, P. (2015). General Systems Theory: It's past and potential. *Systems Research & Behavioral Science*, *32*(5), 514-521.

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal Of Software: Evolution & Process*, *26*(5), 496-503.

Cooper, D. R. & Schindler, P. S. (2006). *Business Research Methods.* New Delhi: Tata McGraw Hill.

Darcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal Of Information Systems*, *20*(6), 643-658.

Darcy, J., Hovav, A. & Galletta, D. (2008). User Awareness of Security Counter measures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 23, 1–20

Dimopoulos, V., Furnell, S., Jennex, M. &Kritharas, J. (2014). *Approaches to IT Security in Small and Medium Enterprises.* Retrieved from http://citeseerx.ist.psu.edu/

Dinev, T., & Qing, H. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386-408.

Fotiou, N., Marias, G.F. & Polyzos, G.C. (2012). *Access Control Enforcement Delegation for Information-Centric Networking Architectures.* Retrieved from http://conferences.sigcomm.org/sigcomm/2012/paper/icn/p85.pdf

Government of Kenya, (2012).*Economic Survey*. Nairobi Kenya: Government Printers.

Government of Kenya, (2013).*Economic Survey*. Nairobi Kenya: Government Printers.

Greener, S.L. (2008). *Business Research Methods*. Copenhagen: Ventus Publishing ApS.

Ibrahim, M. & Ibrahim, A. (2015). The Effect of SMEs' Cost of Capital on Their Financial Performance in Nigeria. *Journal of Finance and Accounting*, *3*(1), 8-11.

ISACA (2011). An Introduction to the Business Model for Information Security. *European Journal of Information Systems, November 2011, Volume 20, Issue 6, pp 643–658*

Johnson, J. C., Leeds, B. A., & Wu, A. (2015). Capability, Credibility, and Extended General Deterrence. *International Interactions, 41*(2), 309-336.

Kankanhalli, A., Teo, H.H., Tan, C.Y. & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kimwele, M., Mwangi, W. &Kimani, S. (2005). Adoption of Information Technology Security Policies: Case Study of Kenyan Small and Medium Enterprises. *Journal of Theoretical and Applied Information Technology, 18*(2), 1-12.

Kothari, C. R. (2004). *Research methodology*: *Methods and techniques*. New Delhi: New Age International (P) Limited Publishers.

Krop, R. (2014). *The Influence of Business Strategies on the Performance of Small and Medium Enterprises in Nairobi County, Kenya.* Retrieved from http://erepository.uonbi.ac.ke/handle/11295/75108

Lee, S. M., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707.

Lejarraga, I., & Oberhofer, H. (2015). Performance of small- and medium-sized enterprises in services trade: evidence from French firms. *Small Business Economics, 45*(3), 673-702.

Lijiao, C., Wenli, L., Qingguo, Z., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers In Human Behavior, 38,* 220-228.

Makumbi, L. K. (2012). *An analysis of Information Technology (IT) security and the adoption of security policies: a case study of Kenyan Small and medium Enterprises (SMEs).* Retrieved from sci.uonbi.ac.ke/print/3454

Mochoge, O.C. (2013). *Determinants of implementation of strategic information systems in small and medium firms.* Retrieved from http://ir.kabarak.ac.ke:8080/

Moorthy, K., Tan, A., Choo, C. & Wei, C.S. (2012). A Study on Factors Affecting the Performance of SMEs in Malaysia. *International Journal of Academic Research in Business and Social Sciences, 2*(4), 224-232.

Mugenda, A.G. & Mugenda, O.M. (2003). *Research methods; Qualitative and quantitative Approaches.* Nairobi: Kenya Acts Press.

Mutandwa, E., Taremwa, N. K., & Tubanambazi, T. (2015). Determinants of Business Performance of Small and Medium Size Enterprises in Rwanda. *Journal of Developmental Entrepreneurship, 20*(1), 1-12.

Nabila, A. (2012). *The Impact of Cyber Security on SMEs.* Retrieved from http://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf

Ngechu, M. (2004). *Understanding the research process and methods. An introduction to research methods.* Nairobi: Acts Press.

Ngura, S., Kimwele, M. &Rotich, G. (2015).Determinants of Information Security among Small and Medium Enterprises in Kenya. *European Journal of Business Management, 2*(1), 124-143.

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.

Opiyo, R. O., & Kakumu, O. A. (2006). ICT Application in the Informal Sector: The Case of the Kariokor Market MSE Cluster in Nairobi. *Urban Forum, 17*(3), 241-261.

Orodho, A. J. (2007). *Techniques of Writing Research Proposal and Reports*. Nairobi: HP Enterprises.

PWC (2011).*Global Information Security 2015: PWC*. Retrieved from www.pwc.com

Quackenbush, S. L. (2010). General Deterrence and International Conflict: Testing Perfect Deterrence Theory. *International Interactions, 36*(1), 60-85.

Republic of Kenya. (2011). *Sessional Paper No. 2 of 2009 on Development of SMEs for Wealth and Employment creation and Poverty Reduction.* Nairobi: Government Printers.

Rui-Feng, Z., Ning, J. & Yu, P. (2012). *Application of role-based access control in information system.* Retrieved from http://ieeexplore.ieee.org/

Sharma, M. K., Bhagwat, R., & Dangayach, G. S. (2008). Performance measurement of information systems in small and medium sized enterprises: a strategic perspective. *Production Planning & Control*, *19*(1), 12-24.

Sharu, H. & Guyo, W. (2015). Factors Influencing Growth of Youth Owned Small and Medium Enterprises in Nairobi County, Kenya. *International Journal of Science and Research, 4*(4), 973-987.

Shen, V. R., Chung, Y., & Chen, T. (2009). A novel application of grey system theory to information security (Part I). *Computer Standards & Interfaces, 31*(2), 277-281

Shin, H., Lee, J., Kim, D., & Rhim, H. (2015). Strategic agility of Korean small and medium enterprises and its influence on operational and firm performance. *International Journal of Production Economics*, *16*(8), 181-196.

Taylor, A., & Taylor, M. (2014). Factors influencing effective implementation of performance measurement systems in small and medium-sized enterprises and large firms: a perspective from Contingency Theory. *International Journal of Production Research*, *52*(3), 847-866.

Tidwell, C.L. (2013). *Testing the Impact of Training with Simulated Scenarios for Information Security Awareness on Virtual Community of Practice Members.* Retrieved from http://etd.fcla.edu/CF/CFE0003566/Tidwell_Craig_L_201105-PhD.pdf

Tomsic, N., Bojnec, S., & Simcic, B. (2015). Corporate sustainability and economic performance in small and medium sized enterprises. *Journal of Cleaner Production*, *10*(8)603-612

Upfold, C.T. & Sewry, D.A. (2008). *An Investigation of Information Security in Small and Medium Enterprises (SME's) In the Eastern Cape*. Retrieved from http://icsa.cs.up.ac.za/

Vijayakumar, U., & Ilangovan, D. (2015). A Quantitative Approach to Information Systems Audit in Small and Medium Enterprises. *Informatica Economica*, *19*(3), 89-95.

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360-365.

Zhi, X. N. & Sean, B. (2013). Information Security Management: Factors that Influence Security Investments in SMEs. *Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan Universit*y, Perth, Western Australia, and 2nd-4th December, 2013.

APPENDICES

Appendix I: Introduction Letter

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

REF: INVITATION TO PARTICIPATE IN A RESEARCH STUDY

I am a student at the Kenyatta University conducting a research project as part of the course requirement for Master of Business Administration. The study seeks to investigate the effect of information technology security practices on the performance of small and medium enterprises in Nairobi County.

This letter serves to kindly request for your co-operation and participation, in a bid to obtain information for the above study. I assure you that the information will be used strictly for academic purposes and all information will be treated confidentially. A copy of the study will be available upon request. Thank you for taking time to participate in the study.

Yours faithfully,

Gladwell Njoki Murigi

Appendix II: Questionnaire

Kindly answer the following questions as truthful and precisely as possible. All the information that you will provide will be kept with strict confidentiality. Also, your responses will be used for academic purposes only. Kindly tick your answers against each questions or write your responses in the spaces provided.

General Information

1. Gender

   Male [ ]

   Female [ ]

2. Age Bracket

   Below 25 Years […] 25 to 35 Years [ ]

   36 to 45 Years [ ] 46 years and above [ ]

3. Highest level of Education?

   Postgraduate [ ] Bachelors [ ]

   Diploma [ ] Certificate [ ]

4. For how long has your business been in operation?

   Less than 2 years [ ] Between 2 - 4 years [ ]

   Between 5 - 7 years [ ] Over 7 years [ ]

Information technology policies

5. Are there formal information technology policies in your business?

   Yes [ ] No [ ]

6. If yes, what is the content of the information technology policy?

   ……

   ……

7. To what extent do information technology policies influence the performance of small and medium enterprises in Kenya?

   To a very Great Extent [ ] Great Extent [ ]

   Moderate Extent [ ] Low Extent [ ]

   No extent at all [ ]

8. To what extent do the following aspects of information technology policies and influence the performance of small and medium enterprises in Kenya? (Where: 1 represents no extent at all, 2 represents low extent, 3 represents moderate extent, 4 represents great extent, 5 represents very great extent)

	1	2	3	4	5
Back up policy					
Policies on access control					
Policies on sharing, storing and transmitting of data					
Privacy and Confidentiality policy					

9. How else do information technology policies influence the performance of small and medium enterprises in Kenya?

……

……

……

Information technology awareness and training

10. Have you or any of your staff ever received training on information technology security?

    Yes [ ] No [ ]

11. To what extent does information technology awareness and training influence the performance of small and medium enterprises in Kenya?

    To a very Great Extent [ ] Great Extent [ ]

    Moderate Extent [ ] Low Extent [ ]

    No extent at all [ ]

12. To what extent do the following aspects of information technology awareness and training influence the performance of small and medium enterprises in Kenya? (Where: 1 represents no extent at all, 2 represents low extent, 3 represents moderate extent, 4 represents great extent, 5 represents very great extent)

	1	2	3	4	5
Security training and education					
Communication channels					
Frequency of training					

13. How else do information technology awareness and training influence the performance of small and medium enterprises in Kenya?

……

……

……

System monitoring and maintenance

14. Does your business monitor and maintain its information technology?

    Yes [ ] No [ ]

15. If yes how often?

    Every week [ ]

    Every month [ ]

    Every 6 months [ ]

    Once in 1 year [ ]

    When there is a perceived threat [ ]

16. To what extent does system monitoring and maintenance influence the performance of small and medium enterprises in Kenya?

    To a very Great Extent [ ] Great Extent [ ]

    Moderate Extent [ ] Low Extent [ ]

    No extent at all [ ]

17. To what extent do the following aspects of system monitoring and maintenance influence the performance of small and medium enterprises in Kenya (Where: 1 represents no extent at all, 2 represents low extent, 3 represents moderate extent, 4 represents great extent, 5 represents very great extent)

	1	2	3	4	5
Frequency of maintenance					

Inspection procedures					

18. How else does security monitoring and maintenance influence the performance of small and medium enterprises in Kenya?

    ……..

    ……..

    ……..

Access control

19. Do you think access control enhances information technology security?

    Yes [ ] No [ ]

20. If yes how?

    ……..

    ……..

    ……..

21. Which of the following access control measures has your business adopted to enhance information technology security?

    Use of passwords [ ]

    Biometric access controls [ ]

    Smart cards [ ]

22. Has your business experience unauthorized access in the last one year?

    Yes [ ] No [ ]

23. To what extent do the following access control measures influence the performance of small and medium enterprises in Kenya? (Where: 1 represents no extent at all, 2 represents low extent, 3 represents moderate extent, 4 represents great extent, 5 represents very great extent)

	1	2	3	4	5
Passwords					
Biometric access controls					
Smart cards					

24. How else does access control influence the performance of small and medium enterprises in Kenya?

……..

……..

……..

Performance of small and medium enterprises

25. To what extent does information technology security influence the performance of small and medium enterprises in Kenya? (Where: 1 represents no extent at all, 2 represents low extent, 3 represents moderate extent, 4 represents great extent, 5 represents very great extent)

	1	2	3	4	5
Sales volume					
Profitability					
Customer satisfaction					
Number of customers					

26. What do you recommend should be done to improve the performance of SMEs in relation to information technology security?

……..