E-COMMERCE SECURITY AND PERFORMANCE OF SMES IN NAIROBI, KENYA

BY

EVA WANJIRU NGUGI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION (MBA), SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

NOVEMBER 2016

DECLARATION

This research project is my original work and has not been presented for award of a degree in any other university.

Signature..... Date.....

EVA W. NGUGI
D61/72802/2014

This research project has been submitted for examination with my approval as a university supervisor

Signature..... Date.....

MR. JOEL LELEI
Lecturer, Department of Management Science:
School of Business, University of Nairobi

DEDICATION

I dedicate this project to my beloved family for their invaluable support both emotional and financial in my pursuit for knowledge. I am greatly indebted to God for the far He has brought me. All glory and honor be to the Most High God who has watched over me and graced me to do this project. I also dedicate this project to my church Renewed Pentecostal Missionary Church for the life lessons that have kept me grounded and sane during this tumultuous journey.

ACKNOWLEDGMENTS

A journey of a thousand miles begins with one step, and as such it has been in my pursuit of knowledge. It has been a long winding road with a few bumps along the way but it was so worth it. It is with utmost sincerity I wish to express my gratitude to the University of Nairobi, for granting me the opportunity to pursue my post graduate degree. I highly appreciate the great efforts of my supervisor Mr. Joel Lelei, for his invaluable support and guidance, who helped navigate the unchartered roads of this journey. I would also like to appreciate the efforts of my mother (Charity), father (Gachau) and brother (Sammy) for their constant words of encouragement albeit a little pressure okay a lot sometimes, but I didn't mind as they had my best interests at heart. I would also like to appreciate my colleagues who accommodated me and covered my duties effectively, special appreciation to Edwin Mukhebi for his assistance in knowledge areas. Last but not least I would like to acknowledge my pastor Passy Kahindo for her spiritual guidance. To all who played a part directly or indirectly my gratitude goes out to you.

God Bless You.

ABSTRACT

E-commerce has been embraced by businesses over time and with the adoption of e-commerce, security challenges have emerged especially those that threaten the continued use of e-commerce platforms. Security threats have been seen as a big impediment to the development of e-commerce. The study sought to identify the most prevalent types of e-commerce security threats faced by SMEs and countermeasures in place to curb the threats. Specifically, the objectives were to determine the challenges faced when managing the threats and to establish a relationship between the types of security threats faced and how they affect organizational performance. The research design used was a descriptive study. The sample size of 100 firms was selected however; responses were obtained from 73 firms. The study used primary data collected by a questionnaire from IT/IS managers using the "drop and pick later" method. The study revealed the most prevalent security threat to be malicious code which includes worms and viruses and the biggest challenge in managing the security threats to be financial constraints. The regression model was used to show the association between the types of e-commerce security threats and organizational performance. The model revealed that there is a notable relation between e-commerce security threats and organizational performance. The study concluded that SMEs ought to understand the types of e-commerce security threats they are most likely to encounter as they have a telling effect on organizational performance and as such cannot be ignored.

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

E-COMMERCE	Electronic Commerce
SME	Small Medium Enterprise
CCK	Communication Commission of Kenya
GDP	Gross Domestic Product
KE-CIRT	Kenya Computer Incident Response Team Coordination Centre
KENIC	Kenya Network Information Centre
KENET	Kenya Education Network
KIPPRA	Kenya Institute for Public Policy Research and Analysis
ICMP	Internet Control Message Protocol
ITU	International Telecommunication Union
TESPOK	Technology Service Providers of Kenya
TPB	Theory of Planned Behaviour
TAM	Technology Acceptance Model
SYN	Synchronised
IPS	Intrusion Prevention Systems
IP	Internet Protocol
IT	Information Technology
USB	Universal Serial Bus
TCP	Transport Control Protocol
UDP	User Datagram Protocol
NCBD	Nairobi Central Business District

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Information technology has largely been adopted by developing countries and is concerned with the development, study, design, implementation, management or support of computer information systems, especially computer hardware and software applications (Kumar, 2014). E-commerce refers to a vast span of online activities and also more specifically to the use of automated transmissions and digital information processing technology to redefine business transactions for value creation in organizations and or individuals (Chanana & Goele, 2012). E-commerce has been plagued by security threats which have evolved with new technological advancements as hackers devise new mechanisms of stealing information (Jebur, Gheysari, & Roghanian, 2012).

The onset of e-commerce instigated studies by various researchers (Nooteboom, 1994; Gessin, 1996; Auger & Gallaugher, 1997) who predicted that Small Medium Enterprises (SMEs) were more plausible to realize the benefit from e-commerce due to their operations in an unknown external environment. Many reasons have been put forward, a key factor being security which has been seen as a constant hurdle to the selection and enforcing of e-commerce for customers and organizations (Antón & Earp, 2000; Suh & Han, 2003). The adoption of e-commerce has significant benefits to organizations but if the security threat remains unchecked, the challenges may far outweigh the advantages. It is therefore crucial for organizations to enforce security measures to guard against known threats.

In Kenya, the government through the CCK established KE-CIRT, the Kenya Computer Incident Response Team Coordination Centre, part-funded by the ITU, which brought together government agencies, the Central Bank and Internet expertise from (KENIC, TESPOK and KENET) to tackle cyber and e-commerce threats as and when they transpire (Souter & Kerrets-Makau, 2012). The 2015 Cyber Security Report prepared by SERIANU and TESPOK revealed that Kenyan firms lost Sh15billion in 2014 through cybercrime.

1.1.1 E-commerce Security

As SMEs adopt e-commerce, more advanced technologies are constantly being developed and improved. The success or failure of operating e-commerce has been linked and not

limited to the business model, team, security of data and storage, customers, product and investors. Therefore for a business to gain competitive advantage in the global market, it is essential that they have a comprehensive security policy with all the stakeholders in place (Al-slamy, 2008).

E-commerce security threats are not centred on one area of e-commerce but instead revolve around various aspects of e-commerce transactions. They are considered as both systems engineering and social issues thus require participation of the entire society (Fu-guo & Yu-jie, 2010). Threats have been classified by various authors. Types of threats have been classified as malicious code attacks which include: viruses, worms, Trojan horses, logic bombs, denial of service attack i.e.-distributed denial of service, SYN Flooding and Phishing (DiYanni, 2012). E-commerce threats are categorised as: web server threats, database threats, reconnaissance, social engineering, port scanning, vulnerability scanning, e-commerce server attacks, physical attacks, malware, and denial of service which small businesses should be cautious against (Rahman & Lackey, 2013).

Security threats are constantly emerging, perpetuated by hackers who devise more ways of carrying attacks faster than security controls can be put in place. Security measures are devised to counter attacks (Revathi, Shanthi, & Saranya, 2015). Several countermeasures have been developed overtime to counter threats arising from e-commerce activities. They include: firewalls- proxy server, routers- network address translation, network intrusion devices - network and host intrusion detection device, authentication -secure sockets layer, encryption - secure shell, tunneling -virtual private networks (Diyanni, 2012). Many of the attacks can be stopped, if detected early enough therefore; a comprehensive countermeasure plan should be in place. Ensuring that service accounts operate with the least privilege, frequent auditing of user accounts, use of stored procedures when possible and use of a web vulnerability scanner are some of the measures that can curb attacks (Lokhande & Meshram, 2013).

Security challenges will remain to be a persistent concern because hackers and attackers are constantly devising new ways of stealing data and information thus posing a perpetual impediment to threat management. Attackers are now also able to take advantage of new vulnerabilities in less time than ever. (GAO, 2003). Since security is not solely based on technology; failure to enforce proper organizational processes, will cause the security

problem to remain unsolved (Treese & Stewart, 1998). According to Anderson (1994), the weak link in security is mostly caused by employee behaviour rather than the adoption of technology. Employees tend to have unlimited access to all the organizational information, depending on the policies that have been put in place. The users are often unable to adhere to security policies or guidelines or are unwilling to comply. They not only lack understanding in what they need to do but they also do not take the necessary precautions for the security enforced to take place effectively (Davis, 1996).

In as much as there is no single perfect security measure, firewalls in many respects have yielded better results than other control mechanisms (Schultz, n.d.). However, Bouchard (2013) contests that the effectiveness of firewall security is diminishing as web applications are being devised that are allowed by security policies. In preventing insider attacks, a detailed insider scenario is developed which involves the accumulated impact of assessment, detection and delay over the response and mitigation will be dependent on the effectiveness of interrupting the malicious act and the subsequent consequences (IAEA, 2008). Valid countermeasures are also provided as add-ons to existing systems which can cause weaknesses as a result of many heterogeneous systems. Since no one countermeasure can guard against all attacks, it is important to identify threats that are specific to your particular scenario and prioritize them based on risk they pose to your organization (Microsoft, 2003).

Numerous small and medium-sized companies are growing more particular to their organizational performance. Organizational performance is defined as the verified results or output of an organization as weighed against its targeted results or outputs. Periodic ill-intentioned security assaults on IT frameworks present a grave danger which necessitates companies to enact the necessary preserves to ensure the confidence, probity, and availability of information. Non fulfilment of appropriate measures renders them susceptible to massive financial sanctions, loss of customer base and goodwill (Sobihah, Embat, Amin, & Muda, 2014).

1.1.2 Small Medium Enterprises (SMEs)

Given the variation of different, sectors, economy and turnover, a single definition is not applicable easily (Vilaseca, 2013). Sessional Paper No. 2 of 2005 expounds an SME as a business which employs between 1 to 50 employees, the World Bank states that an SME is one that falls under one of five of the criteria which says: (1) A formally registered enterprise (2) with an annual yield of between Kenya Shillings 8 to 100 million (3) an asset base of at

least Kenya Shillings 4 million and (5) hiring between 5 to 150 employees. The MSME Bill (2011) uses the criteria to explain SMEs that is: (a) the number of hired labour and (b) the organization's annual yield. For operations in the manufacturing industry, the explanation covers the investment in plant and equipment including the registered capital. They are categorized as: Food, Beverage and Tobacco, Books and Stationery, Energy, Electrical and Electronics, Plastics and Rubber and Pharmaceutical and Medical Equipment.

There are about 90% of SMEs that contribute over 50% of employment worldwide, (Katua, 2014). SMEs are instrumental to economic development by merit of their absolute numbers and rising contribution to employment and Gross Domestic Product (GDP). SMEs form a core pillar of economic activity in Kenya and contribute close to 45% of the GDP which is about 85% of the Kenyan workforce (SME FEST). SMEs are the fastest growing business segment in the economy and employ the most people (50% or 11 million).

SMEs encounter a lot of challenges that considerably hamper their growth and development. They take on the distinctive complications of evolution, riskiness and innovation. The major crucial complications are those of "limited market access, limited access to information, finances and technology and unfavourable policy and regulatory environment among others" (Republic of Kenya, 2010).

1.2 Research Problem

The subject of e-commerce security elicits similar reactions from different stakeholders regardless of their role in the e-commerce process. Consumers of e-commerce and organisations will be concerned with issues of trust, security and privacy. Thus, globally research that was undertaken analysing the effect of e-commerce as experienced by Arab world countries revealed that the level of security and confidentiality perceived by the consumers played a critical role in its adoption. The data collected from companies revealed that issues of security and confidentiality can be overcome by encryption, Trustmark certificates with extended authentication validation (EV) and secure socket layer certificates (Alrawabdeh, Zeglat, & Alzawareh, 2012). In a research conducted in India about online shopping threats, the research found that, consumers were particularly concerned with security during online purchase and therefore organisations which had secured their websites enjoyed more online purchases. They also identified, viruses to be the major threat facing e-commerce users (Niranjanamurthy & Chahar, 2013). The gap exists between developing

countries in that these studies focussed on online payment through e-commerce in large organisations while most developing countries' economies are run by SMEs. There also contextual differences that apply to Kenya and developed countries such as different operating factors like the economy, taxation, social and political factors all of which directly or indirectly influence organisations.

SMEs adoption of e-commerce has increased subsequently over the years, this is in spite of some of the challenges they face of ineffective leadership, financial constraints and uncertain market conditions. Research undertaken on online market place challenges in Kenya, found that online fraud is rampant due to users' lack of awareness of threats, increased use of mobile devices and increased sophisticated attacks. The best practices to curb threats were identified as "robust security systems for detection and prevention of fraud related attacks, continuous detection and conventional protection measures, incident management plans, and regular security assessments" (Kanyaru & Kyalo, 2015, p. 6).

An earlier study posits that failure to implement the basic countermeasures and lack of security policies is why the security problem persists in Kenya (Kimwele, Mwangi, & Kimani, 2013). A Kenyan study conducted on SMEs in the financial sector to identify the most prevalent types of security threats and countermeasures employed, revealed that viruses and system users posed the biggest threat to security and firewalls featured prominently as a countermeasure mechanism (Makumbi, Miriti, & Kahonge, 2012). In yet another research undertaken on tours and travel companies in Nairobi, the study revealed that the main cause of security incidents was virus and malicious code, followed by human errors and lastly software errors (Watuthu, Kimwele, & Okeyo, 2015). The existing gap is the focus on a specific industry which leaves other industries security challenges unexplored. The previous studies focussed on specific categories of the SMEs and thus cannot be used to draw generalizations for all SMEs.

E-commerce security has remained to be one of the pertinent issues facing organisations big and small alike. Due to the unique nature of SMEs however, they do tend to face a rather uphill task of ensuring security is upheld. Consequently, the researcher was keen to address it by focussing on the following questions. What are the types of e-commerce security threats faced by SMEs in Nairobi? What is the effect of e-commerce security on the performance of SMEs? What are the challenges in managing the threats?

1.3 Research Objectives

The overall research objective of the study is to assess e-commerce security threats in SMEs in Nairobi, Kenya. Specifically, the study was directed at the following objectives.

i. To establish the types of e-commerce security threats faced by SMEs in Nairobi.
ii. To determine the effect of e-commerce security on the performance of SMEs.
iii. To establish challenges faced in managing the e-commerce security threats.

1.4 Value of the Study

E-commerce is slowly gaining ground as one of the key ways for SMEs to gain competitive advantage. It has opened up a world of opportunities and possibilities for small business owners to increase their customer base as well as reap all other benefits associated with e-commerce adoption.

This study seeks to add to the body of knowledge of the security threats based on the theory of planned behaviour which will analyse how the SMEs adopt countermeasures and effectively identify and manage security threats. The technology acceptance model will be used to analyse the factors that lead SMEs to adopt different countermeasures. It will carry the assumption that e-commerce threats are known and therefore countermeasures have been enforced. It will assess the relationship between organisational performance and e-commerce security and the challenges in managing the threats as faced by the SMEs in Nairobi will be analysed.

The findings from this research will help scholars and academicians in developing and expanding the syllabus in respect to this study thus providing a deeper understanding of the security threats that SMEs are prone to and their implications. Apart from this, the results of the findings may encourage other researchers to expand their research in the area of e-commerce security. Furthermore, IT consultants may use this information to appropriately design security policies that will be specific to the SMEs in curbing future threats.

The government can use the findings of this research to develop policies of mitigating e-commerce security threats as well as come up with initiatives and provide funding to support the use and development of e-commerce among SMEs.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter analyses literature corresponding to e-commerce security discusses the common security threats to e-commerce in SMEs, the countermeasures enforced to curb the threats, the challenges in countering the threats, the effectiveness of the countermeasures enforced in previous related studies and it further goes on to review the relationship between security and performance of an organisation.

2.1.1 Theoretical Framework

This section documents the relevant theories and literature from similar past studies with consideration to the objectives of the proposed study. It also presents the conceptual framework that underlies the study. The major theories discussed herein are the theory of planned behaviour and the technology acceptance model theory.

2.1.2 Theory of Planned Behavior (TPB)

Ajzen (1991) advanced the Theory of Planned Behavior (TPB) which asserts that the characteristic's behavior is best determined by three constructs. These intentions are predicted by attitudes which are either positive or negative feelings, the subjective norms (a person's perception of how other's beliefs influence their engagement in a distinct behavior) and perceived behavioral control which represents the constraints on behaviour and refers to the 'perceived ease or difficulty of performing behaviour' (Ajzen, 1991, p. 188).

In developing countries, TPB establishes that perceived benefits, accessibility, internet difficulties and management support plays a very great role in its adoption. It can also be inferred that while manager/owner and information systems characteristics may guide the starting decision for the adoption of e-commerce in SMEs, managers may not influence the degree of its subsequent enactment (Shemi, 2012). Therefore, adoption of e-commerce security will largely depend on the attitudes of the perceived advantages and how they have been implemented by other organisations in their field of operation. Managers will also directly or indirectly influence the security measures that a firm will adopt to combat security threats.

2.1.3 Technology Acceptance Model (TAM)

TAM was conceptualized to define the user adoption of technology in organisations. It points out that perceived usefulness and perceived ease of use as the main determinants of system usage in organisations. Although TAM model is popular, it has a negative side of being general and ignorant of personal behavioural factors like social and cultural influences that may be critical in the understanding of e-commerce adoption in developing countries SMEs. The second weakness of TAM arises due to the fact that equating perceived usefulness to use is seen as problematic in some literature. Perceived usefulness is poorly correlated with actual use. Self-reported usage or intention to use may not also be an appropriate alternative for use since users are poor estimators of aspects of their individual behaviours (Shemi, 2012).

Thus in summary, the perception of a technology and its advantages that one has not used is seen as a problem for TAM duplication in developing countries. This is because the prevailing circumstances in the developing countries may not be inevitably the same as the ones in the developed countries (Shemi, 2012). E-commerce security adoption will depend on the system users' assumed ease of use and usefulness to attain a specific goal. Countermeasures to be employed by the firms will have to be perceived as easy to use to be effectively adopted in the organisation. The users should also feel that the measures employed will add value to their daily activities.

2.2 E-commerce Security Threats

Threats have been identified as any potential violation of security which could cause harm or damage (Sen, Ahmed, & Islam, 2015). Often, security issues are associated with different types of cyber-attacks, but according to Turban trust issues specifically personal information sensitivity are the bulk of crucial factors to the success of e-commerce as cited by (Haidari & Pakitani, 2011, p. 15). However, Sen et al., (2015) concluded that technological and malicious code attacks were the most severe threats due to the nature of e-commerce transactions to be carried out on the server level.

The most pertinent issues remain a contentious issue thus, for the purposes of this research; we will focus on the previously identified threats. Threats targeting clients are easily embedded in active content web pages such as a Trojan horse which then cause damage. Threats targeting communication channel occur because the message passes through many

intermediate sources thus can be intercepted and altered resulting in an integrity threat. Threats targeting the server can be crippling to an organisation since most servers are the weakest point of an organisation. Databases that connect to web servers can be hacked and confidential data leaked (Yazdanifard et al., 2011).

Viruses attach themselves to a file and require a host file to cause harm while the program is running and lead to loss of data. Worms replicate themselves through the internet and can spread very quickly leading to loss or theft of data across many resources. Trojan horses are malicious code which masquerade as different programs possibly an e-mail which when accessed, allows the attacker access to the system (Hussain, 2013). Logic bombs are forms of Trojan horses only set to go off at a certain time.

Denial of service attempts to flood the server with excessive amount of data such that access is limited even to the legitimate users. Distributed denial of service involves a hacker writing a program which replicates across thousands of computers known as botnets and attack target systems. SYN flooding occurs during an open session with a customer during the acknowledgment phase, a hacker can send false files causing a crash (DiYanni, 2012). The attacks described affect the system.

The Kenya Cyber security report of 2015 identified top security issues as: social engineering, database breaches, insider threats, poor identity and access management, continuous monitoring and response, vulnerability and patch management, emerging technologies and security automation, inadequate budgets and management support and finally security awareness and training.

2.3 E-commerce Security Threats Countermeasures

While integration of security attributes do not ensure a secure system, they are deemed essential to build a secure system (Gautam, 2014) . The nature of the internet and increasing technical know-how has enabled criminals to develop more sophisticated tools and means to perform cyber-attacks. This has put e-commerce security threat challenge at an all-time high (Jebur et al.,2012) .

ISO 7498-2 Standard lists informs on comprehensive security control measures which include authentication, access control, data confidentiality data integrity and non-repudiation. This is a widely accepted classification by computer security experts (Revathi et

al., 2015). Security measures can be analysed in four categories: deterrence, prevention, detection, and reaction.

Due to the nature of security breaches affecting both system and users it is essential for the users to also uphold a specified conduct in order to curb attacks. SME users should appreciate the importance of security, place value on information, understand the root causes of data breaches, understand the cost and benefits of privacy protection and specify privacy policies in their contracts with suppliers (Lacey & Barry, 2010).

Antivirus: There is a huge volume of malware that can be directed towards a company and numerous attack vectors. Viruses spread through multiple platforms like emails, websites and many others and thus having an antivirus is the best form of defence against these attacks (GFI Software, 2010).

Firewalls: To prevent unauthorised access into a guarded network. This prevents probable susceptible services from penetrating or exiting the network and gives a platform for observing security relevant issues as inspections and alerts which can be enacted on the system (Bouchard, 2013).

Backup and redundant systems: This can have many benefits when things go wrong. Disasters whether natural or human made that can delete information from the system can be countered by having a well-tested backup system that will have the system up and running in a short time (Nabila, 2014).

Policies: These are the basis of all information security programs. There is the need for clearly defined rules and objectives that will assist in the management of security of the e-commerce environment. The policy should be in a manner that allows the operation of the SME to go on easily but with a high security (Hussain, 2013).

2.4 Challenges in Managing E-Commerce Security Threats

Security threats remain to be one of the fundamental challenges faced by organisations since vulnerabilities in assets cannot be completely avoided. Harm to assets which include denial of service, modification of data, interruption and destruction inevitably occurs. Threats however cannot be completely avoided. In part, this is because the existing defence models lack

detailed representation of dynamic threat propagation and instead have an isolated focus on techniques to mitigate threats (Onwubiko & Lenaghan, 2007).

In 2001, the Code Red incident harnessed a buffer overflow in Microsoft Windows Internet Server and infected thousands of computers. Effectively managing threats requires a detailed understanding of security relationships and concepts (Onwubiko & Lenaghan, 2007). SMEs tend to ignore that they need security, they also face financial constraints, and they tend to feel that their enterprise is too small to be affected. They view security as an unnecessary overhead hence don't feel the need to prioritize it and also operate in a high risk environment and tolerate it (Lacey & Barry, 2010).

Organisations also suffer from lack of strategic direction, failure to understand overall influence on the supply chain and a misconception of costs associated with e-commerce (Pease & Michelle, 2003). A common yet often overlooked vulnerability is tolerance of weak passwords which pose a high threat to organisations. Most users also connect to unsecured Wi-Fi hotspots which could create a loophole for a hacker to use their credentials. Failure to update patches on workstations and servers creates another loophole (Lokhande & Meshram, 2013).

Patching is considered to be a very important aspect of security but it is restricted by the sheer volume of the security patches. Users also assume that Microsoft Windows addresses critical security vulnerabilities which is not valid. Patch deployment and security updates are also a challenge especially on reporting the current risk state (Hoehl, 2013). Kenyan SMEs face similar global problems including managers' misconception that security is having a firewall and updating the antivirus software regularly. The refusal to put in place proper management structures also poses a challenge for security management (Kimwele, Mwangi, & Kimani, 2013).

2.5 Effectiveness of the Countermeasures Enforced

Effectiveness of countermeasures enforced are subject to some vulnerabilities. Firewall systems which are the most preferred form of security also incur some design and configuration challenges. Intrusion prevention systems suffer from vulnerabilities such as: under estimation of security capabilities of prevention and detection, focus on performance instead of security and non-defined management policies which include design and

implementation (Lokhande & Meshram, 2013). A study conducted on the effectiveness of evasion techniques against intrusion prevention systems revealed that IPS systems were vulnerable to evasion techniques and combinations. The majority of the detection rates were over 95% however, old evasion techniques were seen to penetrate even the most sophisticated of systems. They concluded that the default configurations were not strict enough to block the attacks masked with evasions (Xynos, Sutherland, & Blyth, 2013).

A study conducted by Imperva on the effectiveness of antivirus undertook a sample of 40 anti-virus software and tested them against 82 malwares. The conclusion of the study was that antivirus products are better at malware detection that redistributes quickly in big samples but new strains leave a window for attacks. The window of attack creates a blind spot because security teams are unaware. A proposed security model has been recommended to handle the blind spot which includes monitoring access of servers, databases and files (Imperva, 2012).

Strong password policy is seen to protect against repeated attacks on a user's account, constant speculative attacks on all user accounts and specific attack guessing founded on the details of the user. However, research conducted to determine effectiveness of passwords concluded that it is misguided for users to use strong passwords since they do not offer defence against password stealing attacks. Therefore a good lockout system i.e. three unsuccessful logins would be a better control measure in a small institution (Florencio, Herley & Coskun n.d.).

2.6 E-commerce Security and Organizational Performance

Information security is used to guard against inescapable security accidents, ensure the continuity of business, and reduce destruction. Businesses recognize security as an important issue, but many lack the understanding of what they should be doing or how it can be achieved. If the organization is not informed on the security protocols it should be enforcing, then it is not able to impart on its employees education about how its intellectual property can be guarded. Therefore, for firms to gain from their security management practices they must have the necessary insights into problems at hand and security management controls within the scope that they can effectively accommodate (PACIS, 2013).

Organizations are required to take on a dynamic approach to security planning and

governance. It is therefore, vital that the governance security be incorporated with the running of the enterprise so as to undertake the issues of information security from an administrative perspective hence making use of its leadership, corporate structures and guidelines for the preservation of informational assets. In addition to regulate risks affiliated with security attacks companies are forced to raise their investments in security technologies such as firewalls, intrusion detection systems, encryption, backup, authentication devices, and access control systems among others (Bose, Luo, & Liu, 2012).

Berghof, a non-governmental organization with operations based in Sri-Lanka, came to the realization of the importance of integrating security into the organizational process because security cuts across issues that impart all dimensions of the organization. They decided to incorporate the administrative staff as a part of the security team because security needs a sufficient overall angle, which cannot be fully ensured without the contribution of administrative staff (Berghof Foundation for Peace Support, 2008).

In line with a survey regulated by CSO magazine, 7596 information security senior authorities of 54 countries argued that security violations are not allied to technology and their main challenge is non-technical issues. The conclusion is that information security is an administrative problem not technical. Another research by CSI/FBI research concluded that in spite the fact that 89% of companies having installed firewalls and 60% of them having user identification, 40% of them still did not report system breaches by intruders. This therefore uncovers an obvious drawback of administration of these systems (Haidari & Pakitani, 2011). Security administration is based on the companies needs and aligns with its objectives. Hence, the liability of its handling and administering should also be regarded as the company's everyday tasks. Information security is a great concern in electronic commerce because a remarkable level of recognized security leads to notable customer satisfaction and trust and a noteworthy level of customer satisfaction can eventually lead to more transaction possibilities and advantage for the businesses (Ebrahimi & Naini, 2012).

2.7 Conceptual Model

The conceptual model provides a lens through which e-commerce security metrics can be measured against organizational performance. The determinants of security and how they influence the organization in terms of contribution to organization, including saving costs,

larger markets, increased sales, reduced costs, time saving, productivity, profitability, and market value (Haidari & Pakitani, 2011).

The study aimed at examining the level to which the independent variable, e-commerce security threats (determined by the different types of threats) affects the dependent variable which is organizational performance (in terms metrics of costs, time, profit margins, larger markets and industry leadership).

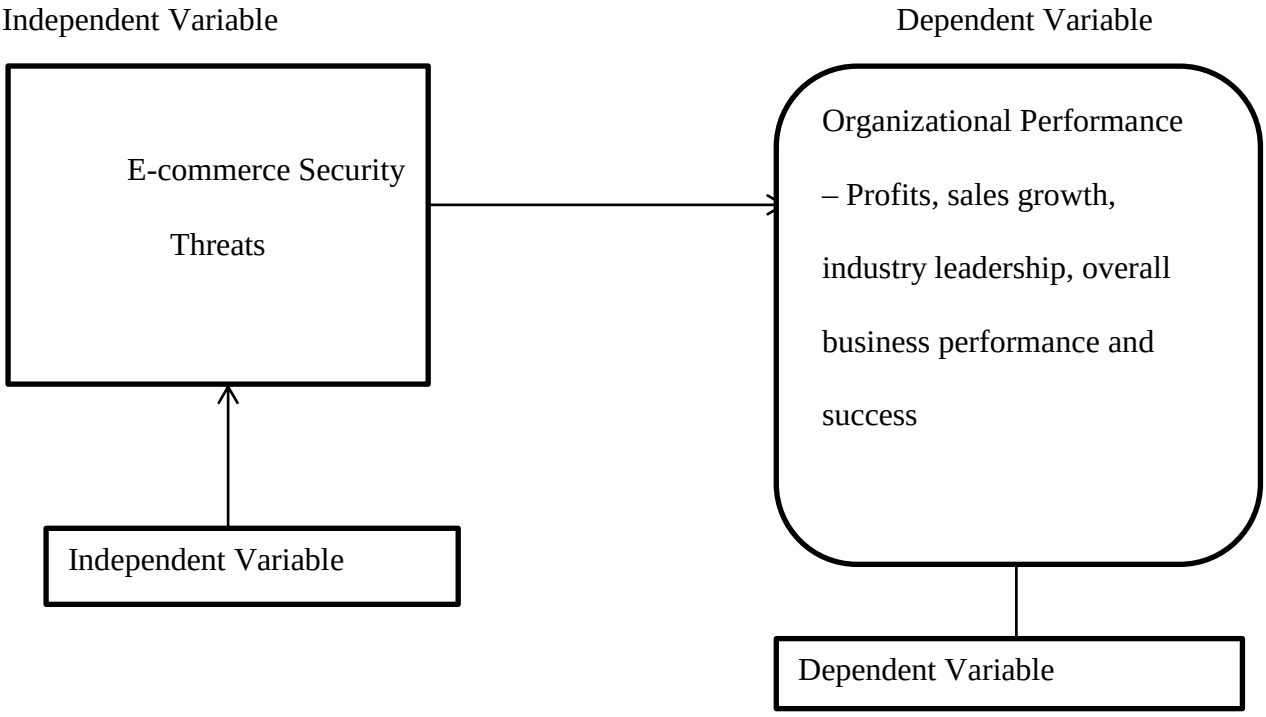

Figure 2.7: Proposed Model for E-commerce Security and Organizational Performance

2.8 Summary of Literature Review

This chapter reviewed literature related to past studies of e-commerce types of security threats and found malicious code and system users to be the leading threats faced by SMEs. While the countermeasures enforced varied, firewalls and antivirus software were seen to be the most preferred countermeasures across a number of SMEs. Whilst challenges in managing security threats differed across different SMEs, financial constraints and lack of management support were constantly seen to be a hindrance to effectively managing the threats. Organizational performance was seen to be influenced by e-commerce security and therefore necessary for inclusion in the management process.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter recounts the approaches that were used by the researcher to collect and analyse data from the field in the study. The section entails: Research design, target population, sample and the sampling procedure, data collection instruments, test of validity and reliability of instruments, data collection procedures and data analysis procedures.

3.2 Research Design

Descriptive research was the research design chosen for the study. Descriptive research is a method that entails accumulating data that defines situations and then organizes, charts, portrays, and outlines the data collection (Glass & Hopkins, 1984). The selection of this design is fitting for this study as it requires administering of a questionnaire as a tool of data collection and helps to establish the determinants of e-commerce security and performance of SMEs in Nairobi, Kenya.

3.3 Population

The study population comprised of formal Small and Medium Enterprises in Nairobi Central Business District. Mugenda and Mugenda (2003), describe a population as a group of individuals or occurrences or entities which share similar observable traits that match a given pattern. According to Muguchu (2010), the Nairobi City County has licensed an estimated 50,000 SMEs operating within the NCBD.

3.4 Sampling

For large populations Cochran (1963), developed a table which is valid where n_0 is the desired sample size, Z is the standard normal deviate at the required confidence level, p is the estimated proportion of an attribute that is present in the population, and q is 1-p, e is the level of statistical significance set. The value for Z is found in statistical tables which contain the area under the normal curve.

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

Confidence interval of 95%, desired level of precision of 5% and assuming p is 7%.

Z=1.96, e=0.05, p=0.07 and q=1-0.07=0.93

Therefore the sample size will be given as:

$$n_0 = \frac{1.96^2 \times 0.07 \times 0.93}{0.05^2} = 100.035 \text{ .}$$

The researcher used sampling method to select a sample of 100 respondents from licensed SMEs registered under the Nairobi City County.

3.5 Data Collection

The principal material of data was primary data. The data collection instrument was a questionnaire. The questionnaires were administered to the IS/IT managers who were respondents for this study due to their knowledge and expertise using the "drop and pick later" method. The questionnaire was subdivided into sections; Section A: comprised of the general information, Section B listed the types of e-commerce security threats, Section C captured the security countermeasures employed to curb security threats, Section D focussed on the challenges in managing security threats and finally, Section E analysed the effect of E-commerce security on performance of SMEs.

3.6 Data Analysis

Upon obtaining feedback from the respondents, the questionnaires were checked for errors then converted to numerical codes representing attributes of variables which are known as coding. The raw data was analysed using SPSS software. Section A which had the demographics was analysed using frequencies and percentages. Section B, C, D was analysed using means and standard deviation while Section E was analysed using regression as it looked to determine the relationship between e-commerce security threats and organizational performance of SMEs.

The regression equation is given as:

Y=a+b1x1+ b2x2+ b3x3

Where: Y is Organisation performance; A is the Y intercept

When X is malicious code; denial of service; social engineering; repudiation; procedural penetration; authentication and privilege attacks; unauthorised access and hackers and attackers, zero b1, b2 and b3 are regression weights attached to the variables.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSIONS

4.1. Introduction

This chapter contains the data analysis results, interpretation and discussion of findings. The overall goal was to examine the type of e-commerce security threats faced by SMEs, the effect of e-commerce security on organizational performance in Nairobi, Kenya, the challenges faced in managing the security threats, the countermeasures enforced to curb the e-commerce security threats and to determine the relationship between types of e-commerce security threats and organizational performance. Data analysis was done using frequencies, mean, standard deviation and regression as the primary tools of analysis. Results are presented in tables and charts.

4.2 Response Rate

The study targeted 100 SMEs located within the NCBD registered under the Nairobi City County. The data was collected from the IS/IT managers because of their knowledge and skill in the area of study. From the table below, 73 out of the 100 targeted SMEs responded to the questionnaire representing a 73% response. This response is considered to be satisfactory and subject to less bias (Ballantyne, 2005) therefore, can be used to make relevant conclusions.

Table 4.2 Response Rate

Respondents	Questionnaires distributed	Questionnaires filled and returned	Response rate
IT/IS Managers	100	73	73
Total	100	73	73

Analysis was done per background information lists objectives as gender, job designation, highest level of learning, type of enterprise, age of the business and duration of use of e-commerce.

4.3 Background Information

The study sought to find out the demographic information based on gender, job level, age, the highest level of education, type of enterprise, age of the business, duration of e-commerce use and category of business operations. The analysis used the results to draw some conclusions.

4.3.1 Position in the Organisation

The study attempted to find out the positions held by the various employees in the organization. The results illustrate that majority of the respondents were in middle management at 45.21% followed closely by senior management at 42.47% and lastly junior management at 12.33%. This is adequate as the managers were vastly equipped with knowledge on the study area. The findings were as shown in the Figure 4.3.1

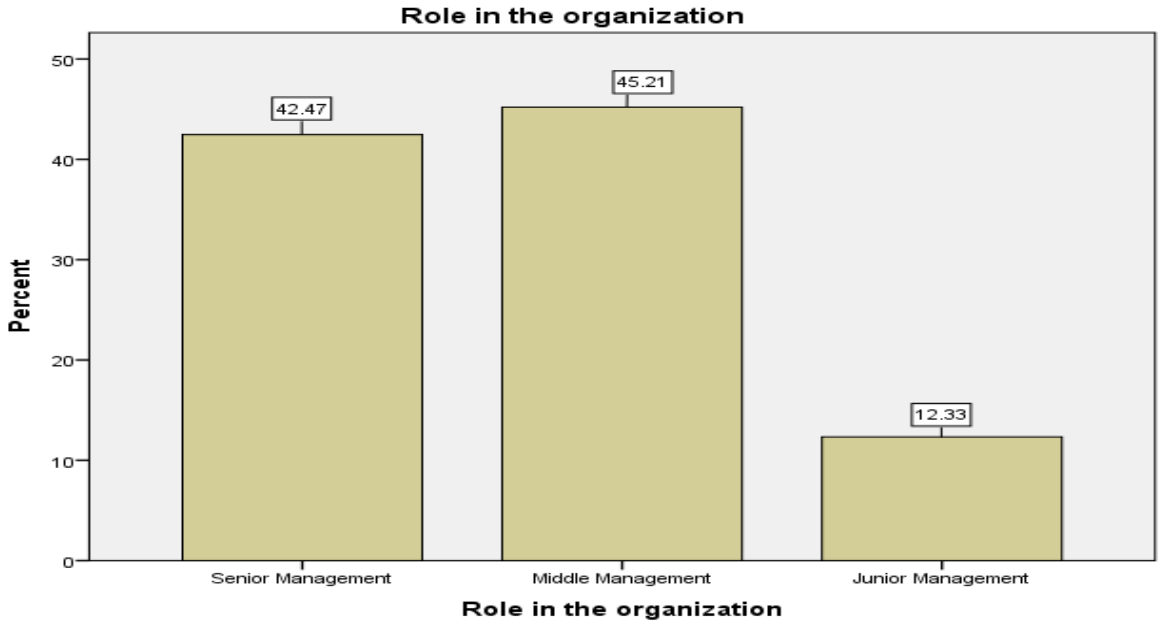

Figure 4.3.1 Role in the Organisation

4.3.2 Gender

The respondents were asked to indicate their gender. The results indicate that most of the respondents were male. However, the female representation is still adequate. The male respondents registered a high percentage of 65.75% while the females were fewer at 34.25%. The findings were as shown in the Figure 4.3.2

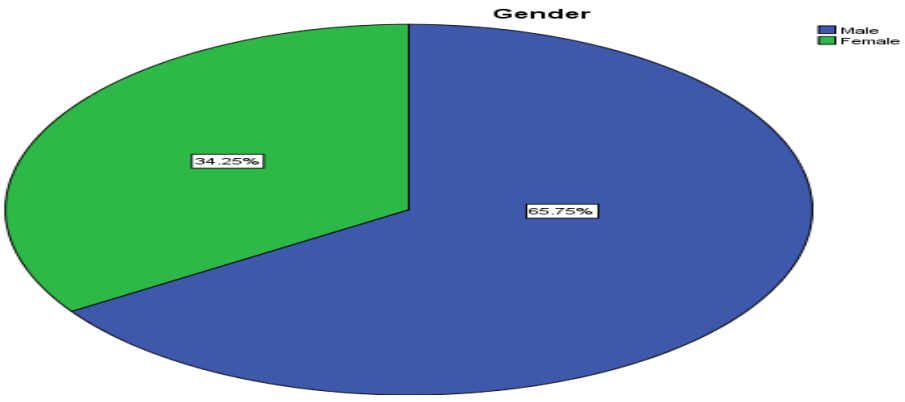

Figure 4.3.2 Gender

4.3.3 Age Group

The study sought to establish the age group of the respondents and the results illustrated that majority of the respondents were between 31-35 years (38.36%) followed by 36-40 years (24.66%), 26-30 years (20.55%) and finally over 40 years (16.44%). The findings were as represented in the Figure 4.3.3

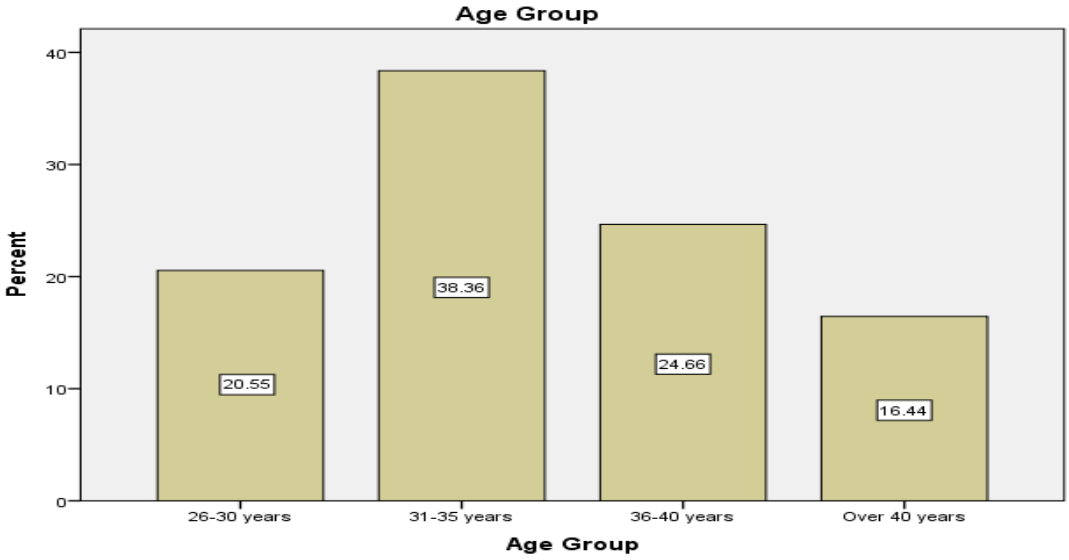

Figure 4.3.3 Age Group

4.3.4 Highest Education Level

The study attempted to establish the highest level of education attained by the various respondents so at to determine their capacity to understand and adequately respond to the questions. The results illustrated that 86.30% of respondents had attained university level education while 13.7% of respondents had attained a college level education. The findings were as shown in the Figure 4.3.4

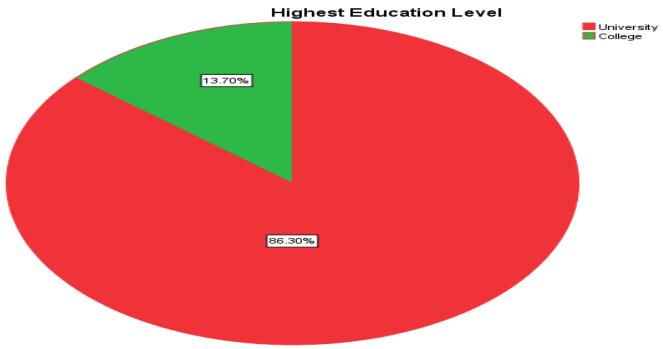

Figure 4.3.4 Highest Education Level

4.3.5 Type of Enterprise

The study attempted to determine the type of enterprise the businesses were. The respondents were asked to indicate the type of enterprise their business was classified as. Majority of the enterprises were private limited companies at 46.58% followed by Sole proprietorships and Partnerships both at 20.55% and lastly public limited companies at 12.33%. The results indicate participation from different enterprises thus results are general and can be applied to these enterprises. The findings were as displayed in the Figure 4.3.5

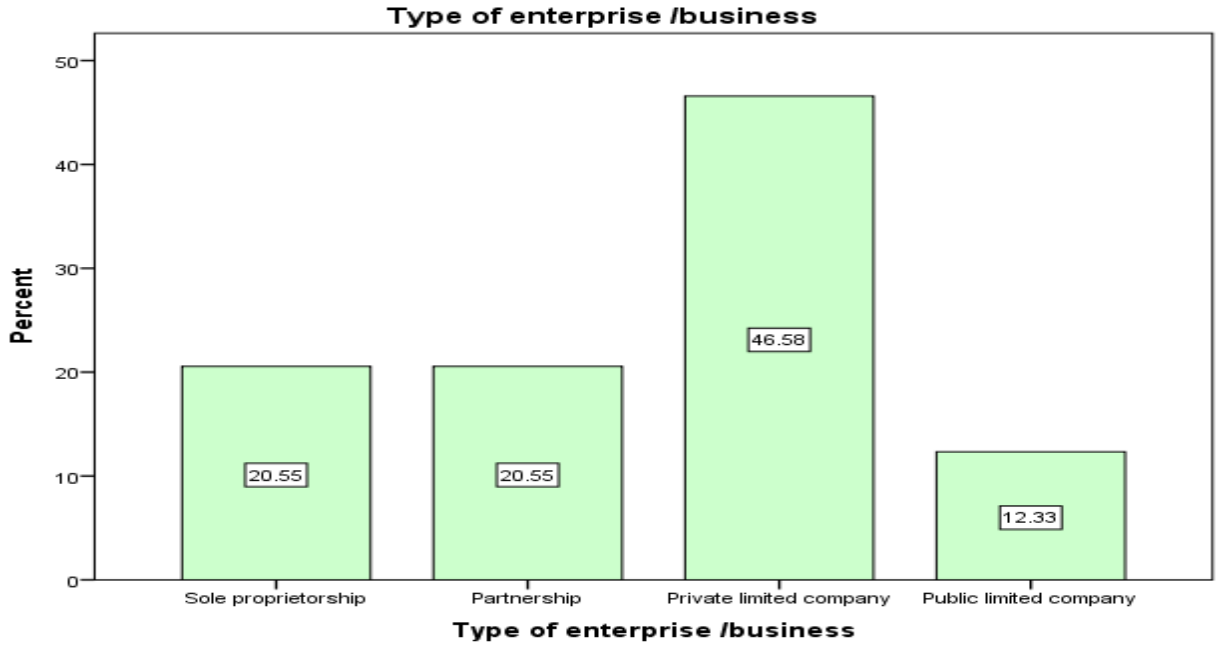

Figure 4.3.5 Type of Enterprise/Business

4.3.6 Age of the Business

The study also attempted to establish the number of years the business has been in operation. The results show that majority of the businesses were between 6-10 years (45.21%) followed closely by 5 or below years (42.47%), few between 11-15 years (8.2%) and finally above 20 years (4.1%). This indicates that the businesses can be used for the study since they have established their operations. The findings are shown in Figure 4.3.6

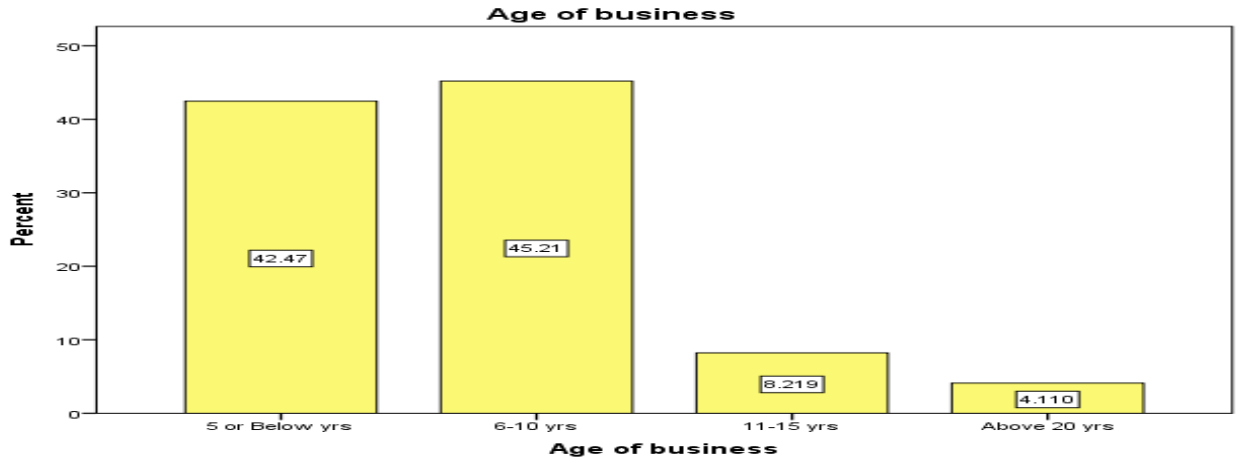

Figure 4.3.6 Age of Business

4.3.7 Category of the Business

The study also attempted to find out the category which best describes the business. The respondents were asked to indicate the category which best describes them. The results indicate a representation of several industries from which generalizations can be drawn.

Table 4.3.7 Category of the Business

Category best describing the business/enterprise

	Frequency	Percent	Valid Percent	Cumulative Percent
Food, Beverage and Tobacco	9	12.3	12.3	12.3
Books and stationery	3	4.1	4.1	16.4
Energy, Electrical and Electronics	27	37.0	37.0	53.4
Pharmaceutical and Medical Equipment	3	4.1	4.1	57.5
Construction	3	4.1	4.1	61.6
Law firm	6	8.2	8.2	69.9
Supplies	13	17.8	17.8	87.7
Spares and hardware shop	3	4.1	4.1	91.8
Advertising	6	8.2	8.2	100.0
Total	73	100.0	100.0	

4.3.8 Duration of E-commerce Use

The study also attempted to find out the length of time which the business has used e-commerce. The results illustrate that majority of the businesses have used e-commerce for 5 or below years (54.79%), followed by 6-10 years (36.99%) and lastly 11-15 years (8%). These results indicate an adequate duration to test the objectives. The findings are shown in Figure 4.3.8.

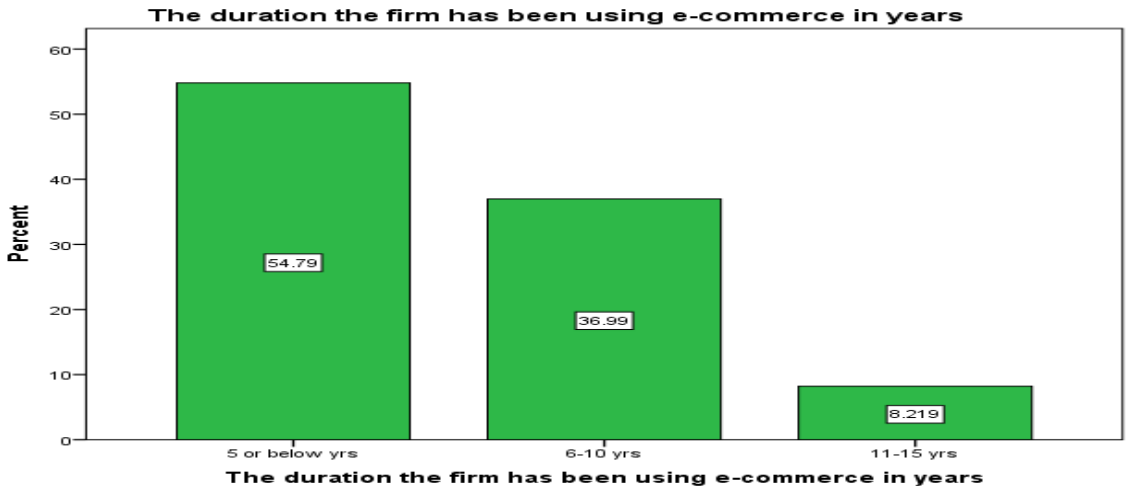

Figure 4.3.8 Duration the firm has been using e-commerce

4.3.9 Likelihood of Future E-commerce Use

The study also attempted to find out the likelihood that the business will continue to use e-commerce. The respondents illustrated willingness to continue use of e-commerce with 83.56% response as very likely to continue and 16.44% likely to continue as shown in the Figure 4.3.9

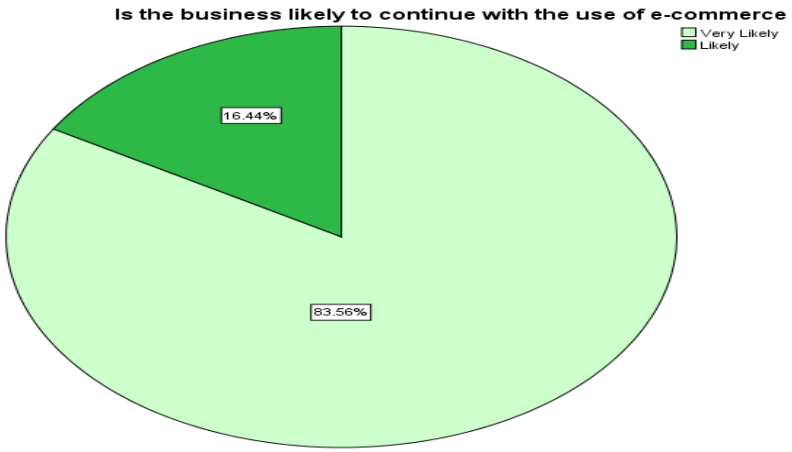

Figure 4.3.9 Likelihood of Future E-commerce use

4.4 Types of E-commerce Security Threats

The study also attempted to find out the extent to which e-commerce security threats have been faced by organizations. The respondents were requested to rate their responses on a Likert scale where 5= to a very large extent 4= Large extent 3= moderate extent 2= small extent 1=no extent. The means and standard deviation were determined and mean scores were interpreted using the scale where; 1-1.4 =no extent; 1.5-2.4=small extent; 2.5-3.4= moderate extent; 3.5-4.4=large extent; 4.5-5=very large extent. The findings were as shown in the Table 4.4.

Table 4.4 Types of E-commerce Security Threats

Types of security threats	N	Mean	Std. Deviation
Malicious code: viruses and worms as a security threat	73	2.97	1.067
Denial of service as a security threat	73	2.32	.643
Social engineering as a security threat	73	2.37	.697
Procedural penetration as a security threat	73	1.86	.933
Hackers and attackers as a security threat	73	1.99	1.047
Unauthorized access as a security threat	73	1.86	.887
Authentication and privilege attacks as a security threat	73	1.90	.960
Repudiation as a security threat	73	2.00	.957

The results calculated from SPSS shows that most of the SMEs recognize malicious code which includes worms and viruses as a moderate threat represented by a calculated mean of 2.97 and a standard deviation of 1.067 this is derived from the 73 enterprises that took part in the study. Procedural penetration represented by a calculated mean of 1.86 and standard deviation 0.933 and unauthorized access represented by a calculated mean of 1.86 and a standard deviation of 0.887 results indicate that the respondents agree only to a small extent of its impact on security as they registered, the least mean scores.

4.5 Security Countermeasures to Curb Security Threats

The study also attempted to find out the extent to which countermeasures have been employed by organizations to curb e-commerce security threats. The respondents were requested to rate their responses on a likert scale where 5= to a very large extent 4= Large extent 3= moderate extent 2= small extent 1=no extent. The means and standard deviation were determined and mean scores were interpreted using the scale where; 1-1.4 =no extent; 1.5-2.4=small extent; 2.5-3.4= moderate extent; 3.5-4.4=large extent; 4.5-5=very large extent. The findings were as shown in Table 4.5.

Table 4.5 E-commerce Security Countermeasures

Security Countermeasures to curb security threats	**N**	**Mean**	**Std. Deviation**
Antivirus as a countermeasures	73	4.10	.915
Role separation as a countermeasures	73	2.97	.745
Backup and redundant systems as a countermeasures	73	2.92	.909
Security policies as a countermeasures	73	2.70	.938
Security awareness as a countermeasures	73	2.74	1.131
Password policies as a countermeasures	73	3.03	1.178
Updates and patches as a countermeasures	73	2.71	1.099
Firewalls as a countermeasures	73	2.75	1.090
Encryption as a countermeasures	73	2.53	1.226

The results calculated from SPSS shows that most of the SMEs have deployed antivirus to counter worms and viruses represented by a calculated mean of 4.10 and a standard deviation of 0.915 which implies that respondents agreed to a large extent to the use of antivirus in curbing threats. Password policies followed represented by a calculated mean of 3.03 and a standard deviation of 1.178 implies that respondents agree to a moderate extent of its importance in security. Further, respondents agreed to a moderate extent on effect of role separation represented by a calculated mean of 2.97 and standard deviation of 0.745 and backup and redundant systems especially for database and servers represented by a calculated mean of 2.92 and standard deviation of 0.909 of employing these measures to counter threats.

Encryption which transforms plain text into cipher text represented by a calculated mean of 2.53 and a standard deviation of 1.226 implies that the respondents agreed to a moderate extent of the necessity to counter threats although it registered the lowest mean score.

4.6 Challenges in Managing Security Threats

The study also attempted to find out the extent to which the organization faced challenges in managing the threats. The respondents were requested to rate their responses on a Likert scale where 5= to a very large extent 4= Large extent 3= moderate extent 2= small extent 1=no extent .The means and standard deviation were determined and mean scores were interpreted using the scale where; 1-1.4 =no extent; 1.5-2.4=small extent; 2.5-3.4= moderate extent; 3.5-4.4=large extent; 4.5-5=very large extent. The findings were shown in Table 4.6.

Table 4.6 Challenges of Managing Threats

Challenges of managing security threats	N	Mean	Std. Deviation
Financial Constraints as a challenge of security threat	73	2.67	.898
Lack of strategic direction as a challenge of security threat	73	2.22	.917
Weak Passwords as a challenge of security threat	73	2.29	1.02
Complexities of security policies as a challenge of security threat	73	2.41	.814
Lack of competent IT personnel as a challenge of security threat	73	2.51	.915
Misconception of e-commerce costs as a challenge of security threat	73	2.30	.681
Emerging Technologies as a challenge of security threat	73	2.55	.708
Users refusal/ inability to comply to set guidelines as a challenge of security threat	73	2.33	.800
Unawareness that they are potential targets as a challenge of security threat	73	2.22	.917
Lack of understanding of security as a whole as a challenge of security threat	73	1.81	.923

The results calculated from SPSS reveals that most of the SMEs face financial constraints represented by a calculated mean of 2.67 and a standard deviation of 0.898 which implies that respondents agreed to a moderate extent to the financial challenge in managing threats. Emerging technologies represented by a calculated mean of 2.55 and standard deviation of 0.708 and the lack of competent IT personnel represented by a calculated mean of 2.51 and standard deviation of 0.915 implies that respondents agreed to a moderate extent of their significance in managing threats as they pose considerable challenges. Lack of understanding of security as a whole represented by a calculated mean of 1.81 and a standard deviation of 0.923 implies that the respondents agreed to a small extent of the impediment posed but only to a minimal extent.

4.7 Effect of E-commerce Security in Performance of SMEs

The study also looked to find out the level to which e-commerce security affected performance by organizations. The respondents were requested to rate their responses on a Likert scale where 5= to a very large extent 4= Large extent 3= moderate extent 2= small extent 1=no extent. The means and standard deviation were determined and mean scores were interpreted where; 1-1.4 =no extent; 1.5-2.4=small extent; 2.5-3.4= moderate extent; 3.5-4.4=large extent; 4.5-5=very large extent. The findings were represented in Table 4.7.

Table 4.7 Effect of E-commerce Security on Organizational Performance

	N	Mean	Std. Deviation
Profitability as organizational performance	73	3.67	.746
Cost Savings as organizational performance	70	3.40	.710
Time savings as organizational performance	73	3.30	.938
Increased sales as organizational performance	73	3.36	1.005
Industry leadership as organizational performance	73	2.85	.811
Market value as organizational performance	73	2.97	.942
Overall business performance and success as organizational performance	73	3.03	.942

The results calculated from SPSS reveals that most of the SMEs view profitability as the measure of organizational performance most influenced by e-commerce security represented by a calculated mean of 3.67 and a standard deviation of 0.746 which implies that respondents agreed to a large extent e-commerce security's contribution to organizational performance. However, industry leadership represented by a calculated mean of 2.85 and a standard deviation of 0.811 implies respondents agreed to a moderate extent of the impact on performance and this aspect of organizational performance registered the least mean score.

4.8 Regression Analysis

A regression analysis was carried out to test association among variables (independent) on the organizational performance of SMEs.

4.8.1 Relationship between Types of E-Commerce Security Threats and Performance of SMEs

4.8.1.1 Test of Co-efficient

The test was carried out to determine whether there was a relationship between types of e-commerce security threats and performance of SMEs. The multiple linear regression models indicate that the independent variables have a negative coefficient. The regression results above show the existence of a negative association between dependent variable and independent variable. This concludes that a rise in the independent variable will cause a decline in the dependent variable.

According to the regression equation, taking all factors (repudiation, hackers and attackers, malicious code, denial of service, social engineering, procedural penetration, and unauthorized access, authentication and privilege attacks) constant at zero, firm performance realized would be 2.955. From the findings, malicious code results to 0.288 decreases in SME performance. Denial of service results to 0.126 decreases in SME performance. Social engineering results to 0.095 decreases in SME performance. Procedural penetration result to 0.13 decreases in SME performance. Hackers and attackers result to 0.264 units decrease in SME performance. Unauthorized access results to 0. 056 units decrease in SME performance. Similarly authentication and privilege result to 0.179 decreases in SME performance. Repudiation results to 0.326 decreases in SME performance. The significant values represented imply that only four variables (malicious code, repudiation, denial of service and hackers and attackers) are the predictors used which were significant. Similarly, the sample

used Z-statistic represented by **t** since it is more than 30. Four of the **t** values are > 1.96 hence only four values are significant (malicious code, repudiation, denial of service and hackers and attackers.

Table 4.8.1.1: Co-efficients

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	2.955	.288		10.274	000
Malicious code: viruses and worms as a security threat	-.288	.078	.483	3.707	000
Denial of service as a security threat	-.126	.136	-.128	-.932	355
Social engineering as a security threat	-.095	.121	-.105	-.791	432
Procedural penetration as a security threat	-.131	.109	.192	1.200	235
Hackers and attackers as a security threat	-.264	.087	-.435	3.035	003
Unauthorized access as a security threat	-.056	.120	-.079	-.471	639
Authentication and privilege attacks as a security threat	-.179	.111	-.270	-1.614	112
Repudiation as a security threat	-.326	.087	.490	3.759	000

a. Dependent Variable: Performance

As per the SPSS generated in Table 4.6, the regression is:

$Y=2.955 + -.288 X_1 + -.126 X_2 + -.095 X_3 + -.131 X_4 + -.264X_5 + -.056X_6 + -.179X_7 + -.326X_8$

4.8.1.2 Model Summary

From Table 4.8.1.2, the coefficient of determination is 41.2%. This indicates that 41.2% of the variation in performance is defined by the differences in the independent variables (types of e-commerce security threats). It represents a fairly good fit and generally accepted as the threshold for a good fit.

Table 4.8.1.2: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.642[a]	.412	.338	.51789

a. Predictors: (Constant), Repudiation, Hackers and attackers, Malicious code, Denial of service, Social engineering, Procedural penetration, Unauthorized access, Authentication and privilege attacks.

4.8.1.3 ANOVA

The F calculated at 5% level of significance was 5.597 since F calculated is greater than the F critical (value = 2.17), this shows that the overall model was significant. The F significance value of 0.00, indicates that regression model has probability of 0% of giving wrong prediction. It can be concluded that regression model is statistically significant, hence suitable for explaining how types of e-commerce security threats affects performance of SMEs.

Table 4.8.1.3: ANOVA[a]

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	12.008	8	1.501	5.597	.000[b]
Residual	17.165	64	.268		
Total	29.173	72			

a. Dependent Variable: Performance

b. Predictors: (Constant), repudiation, hackers and attackers, malicious code, denial of service, social engineering, procedural penetration, unauthorized access, authentication and privilege attacks

4.9 Discussions of the Findings

The types of e-commerce security threats faced by most SMEs revealed that malicious code which includes worms and viruses are the leading types of e-commerce security threats which lead to security incidents in the SMEs. These findings correlate with a study conducted on tours and travel companies which found that malicious code was the leading cause of security incidents in those organisations (Watuthu, Kimwele, & Okeyo, 2015). Social engineering registered a slightly higher threat level than denial of service attacks which shows an emergence of a new threat that SMEs should be aware of and protect themselves against.

The countermeasure employed by most SMEs in countering known security threats is the antivirus. These results show a shift in security countermeasures employed contrary to a previous study on SMEs in the financial sector that found that firewalls were the most prominent countermeasure employed by most SMEs to curb threats (Makumbi, Miriti, & Kahonge, 2012). The use of firewalls has declined significantly with SMEs focussing on the use of antivirus software and password policies. The findings show that with increased vulnerabilities from malicious code and denial of service attacks, countermeasures employed are shifting to accommodate change in threats.

Organization performance is affected by e-commerce security positively when there is a perception of increased security and negatively when faced by security threats. Most SMEs attribute profitability of their businesses to e-commerce security and also enjoyed reduced costs of operations as a result of e-commerce security. SMEs rely on e-commerce platforms for business operations which make it crucial for them to invest in security controls that guard against known vulnerabilities and integrate security processes to their everyday organization activities. These results correlate to previous studies on the importance of data protection from e-commerce security threats which could lead to enormous amounts of loss through data, theft and damage (Ebrahimi & Naini, 2012). Financial constraints were seen to greatly impede e-commerce security adoption which is similar to findings conducted in 2012 on the Kenyan financial sector SMEs (Makumbi, Miriti, & Kahonge, 2012).

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter entails the summary of the findings and conclusions. It also gives the recommendations, limitations and suggestions for further study. This study was undertaken to determine the relationship of e-commerce security threats and organizational performance of SMEs in Nairobi, Kenya. The study had three objectives: to determine the type of e-commerce security threats faced by SMEs in Nairobi, Kenya, to determine the association between e-commerce security threats and organizational performance of SMEs and to establish the challenges faced in managing the e-commerce security threats of SMEs in Nairobi, Kenya. This chapter presents the summary of findings for the three objectives mentioned above, the conclusions, limitations, recommendations made based on findings and the suggestions on areas that need to be researched as far as this study is concerned.

5.2 Summary of Findings

The study established that most SMEs that operate in Nairobi, Kenya have been in existence between six to ten years. Majority of SMEs consider malicious code to be most common type of e-commerce security threat they face and thus have employed the use of antivirus as a countermeasure to withstand attacks. According to a UK study, viruses and worms are responsible for the largest number of security incidents accounting for approximately 41% during 2002 and this is despite the fact that these SMEs have anti-virus software in place (DTI; PriceWaterHouseCoopers, 2002). Majority of the SMEs also listed financial constraints as the main challenge in managing e-commerce security threats. A study conducted in Australia revealed that SMEs are unlikely to revisit information security until after an incident due to the limited budget and are more likely to focus resources on their core business (Ng, Ahmad, & Maynard, 2013).

On malicious code which includes worms and viruses which SMEs recognized as the security threat they were most prone to, the results show that organizational performance is affected which leads to loss of profitability, time, costs and overall business performance. The SMEs agreed that denial of service attacks, social engineering, procedural penetration, hackers and

attackers, unauthorized access, authentication and privilege attacks and finally repudiation only affect their enterprises to a minimal extent. However, the individual impact of each threat to organizational performance shows that malicious code, social engineering, denial of service attacks and finally hackers and attackers have significant effects to organizational performance. These results are in line with a study conducted by Price Water House Coopers (2011), which found that SMEs in the UK experienced malicious code attacks as the highest security vulnerability. Another study also observed a decreased number of denial of service attacks since 2013 (PWC, 2015).

The results also show that financial constraints pose the greatest challenge among majority of the SMEs in managing the e-commerce security threats. Emerging technologies and lack of competent IT personnel also pose a significant challenge to security threat management by SMEs. The lack of strategic direction, weak passwords, complexities of security policies, unawareness of being potential targets and users' refusal to comply to set guidelines were viewed by SMEs as less impacting challenges on threat management.

It is also clear from the study that the eight independent variables of e-commerce security threats negatively affect organizational performance; greatly on profitability; savings, decreased sales, lost market value and overall business performance and as such need to be mitigated while industry leadership is the least impacted variable in organizational performance.

5.3 Conclusions

The study concludes that SMEs in Nairobi, Kenya face malicious code as the most prevalent e-commerce security threat. There is need for the SMEs to be aware of the different types of threats they are prone to and ways of countering attacks by being educated on the same through training sessions in their companies. Countermeasures will be effective only when the specific type of threats prone to the organization is identified. Failure to effectively mitigate these threats results in declined organizational performance. This is supported by the results from a regression analysis conducted that indicated that there is a strong relationship between organizational performance and e-commerce security threats. However, financial constraints limit SMEs from managing threats effectively.

5.4 Recommendations

The study recommends that SMEs should be educated on the types of vulnerabilities they are exposed to as a result of engaging in e-commerce by organising training sessions which should include all users in the organisation. They should then adopt the necessary countermeasures to counter the already identified threats. The study further recommends that SMEs should make investments towards improving the budget allocated for the security.
SMEs should also make investments towards hiring or making their IT personnel more knowledgeable and skilled in all security aspects of the firm. This will also help them to address emerging technologies by being informed of new technological advancements hence keeping up to date with the security trends and thus remain competitive.

SMEs should constantly review security policies so at to minimise risk devastation in case of a security threat and have properly laid down structures and guidelines of how to recover data in case of an attack in the least time possible. They should also carry out penetration testing to identify vulnerabilities in their system. They government should also rally behind them seeing as they contribute to half of the country's GDP so as to reduce the financial burden by creating an environment that promotes innovation and creativity for SMEs.

5.5 Limitations of the Study

The study was subject to some limitations that should be considered when interpreting the study results. First the study focused on SMEs in Nairobi only as registered under the Nairobi City County and secondly this study did not include all categories of SMEs. The study has determined the types of e-commerce security threats and their impact on organizational performance of SMEs in Nairobi, Kenya. The SME trade in Kenya consists of different enterprises which differ in administrative style and organizational culture. Another study should be carried out which encompasses all sectors thus generalization of findings for all SMEs in Nairobi and Kenya can be drawn and hence pave way for new investments in e-commerce security**.**

5.6 Suggestions for Further Research

The study therefore, recommends further study to be carried out to investigate the effectiveness of countermeasures employed in curbing threats in Kenyan SMEs and to also further this study in large enterprises.

REFERENCES

Ahmad, A. (n.d.). Type of Security Threats and It's Prevention. *International Journal Computer Technology & Applications*.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behaviour and Human Decision Processes*, 179-211.

Alrawabdeh, W. A., Zeglat, D., & Alzawareh, A. (2012). The Importance of Trust and Security Issues in E-Commerce Adoption in the Arab World. *European Journal of Economics, Finance and Administrative Sciences*(52), 173-177.

Al-slamy, N. M. (2008). E-commerce Security. *IJCSNS International Journal of Computer Science and Network 340 Security, 8*(5), 340-344.

Anderson, R. (1994). *Why Cryptosystems Fail* (Vol. 37). Communications of the ACM.

Anton, A., & Earp, J. (2000). Strategies for developing policies and requirements. In P. p. e-commerce (Ed.), *CCS2000.*

Auger, P., & J.M, G. (1997). Factors affecting adoption of an internet-based sales presence for small businesses. *The Information Society, 13*(1), 55-74.

Ballantyne, C. (2005). Moving student evaluation of teaching online: reporting pilot outcomes and issues with a focus on how to increase student response rate. *Australasian Evaluations Forum: University Learning and Reaching: Evaluating and Enhancing the Experience*.

Banday, T., & Qadri, J. A. (2007). Phishing- A growing threat to E-commerce. *The Business Review, 12*(2), 76-83.

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational Research: Determining Appropriate Sample Size in Survey Research. *Information Technology, Learning, and Performace Journal, 19*(1), 43-50.

Berghof Foundation for Peace Support. (2008). *Reflecting on Risk and Security Management.* Retrieved from http://www.berghof-foundation.org/: http://www.berghof-foundation.org/fileadmin/redaktion/Publications/Other_Resources/SL_Reflecting_on_Risk_and_Security_Management.pdf

Blakely, B. (2002, February 6). Consultants can offer remedies to lax SME security. *TechRepublic*.

Bose, R., Luo, X., & Liu, Y. (2012). *The Relationship between Information Security Investment and Organizational Performance: a critical review.* Retrieved from http://www.nedsi.org/: http://www.nedsi.org/proc/2013/proc/p121026006.pdf

Bouchard, M. (2013). *Next Generation Firewalls.* Ναυτεμπορικη, 803.

Brake, J. (2003, August 14). Small business security needs for the changing face of small business. *Micro and Home Business Association*.

Cochran, W. (1963). Sampling Techniques. New York: John WIley and Sons, Inc.

Davis, D. (1996). Compliance defects in public-key cryptography. *Proceedings of the 6th usenix Security Symposium*, (pp. 171-178).

Dimopoulos, V., Furnell, S., Jennex, M., & Kritharas, I. (2004). *Approaches to IT Security in Small and Medium Enterprises.* Retrieved May 28, 2016, from semanticscholar.org: https://www.semanticscholar.org/paper/Approaches-to-IT-Security-in-Small-and-Medium-Dimopoulos-Furnell/6c37279a3ae5ae8371cfa232caa622757ff89a9c

DiYanni, B. (2012). E-Commerce: Attacks and Preventative Strategies. *Journal of Chemical Information and Modeling,*.

DTI; PriceWaterHouseCoopers. (2002). *Information Security Breaches Survey.* URN 02/318.

Ebrahimi, A., & Naini, P. (2012). Exploring the Type of Relationship between Information Security Management and Organizational Culture (Case Study in TAM Iran Khodro

Co.). *International Journal of Information, Security and Systems Management, 1*(1), 21-28.

Florencio, Herley, & Coskun. (n.d.). *Do Strong Web Passwords Accomplish Anything?* Retrieved May 28, 2016, from www.usenix.org: https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/florencio/florencio.pdf

GAO (2003). *Effective Patch Management is Critical to Mitigating Software Vulnerabilities.* United States General Accounting Office.

Gautam, A. (2014). Network Security Issues in e-Commerce. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(3), 130-132.

Gessin, J. (1996). *Impact of Electronic Commerce on Small and Medium Sized Enterprises Management.*

GFI Software. (2010). *Security Threats: A guide for small and medium enterprises.* GFI.

Grandon, E., & Pearson, J. (2004). Electronic commerce adoption: an empirical study of small and medium US businesses. *Information & Management, 42*(1), 197-216.

Haidari, A., & Pakitani, K. (2011). *A study about trust and security within E-commerce.* University of Gothenburg, Department of Applied Information Technology.

Hoehl, M. (2013). *Framework for building a Comprehensive Enterprise Security Patch Management Program.* Retrieved 6 8, 2016, from https://www.sans.org: https://www.sans.org/reading-room/whitepapers/threats/framework-building-comprehensive-enterprise-security-patch-management-program-34450

Hussain, A. (2013). A study of information security in e-commerce applications. *International Journal of Computer Engineering Science, 3*(3).

IAEA. (2008, September). Preventive and Protective Measures Against Insider Threat. *8*. Vienna, Austria.

Imperva. (2012). *Assessing the Effectiveness of Antivirus Solutions.* Hacker Intelligence Initiative.

Jebur, H., Gheysari, H., & Roghanian, P. (2012). E-commerce reality and controversial issue. *International Journal of Fundamental Psychological and Social Sciences, 2*(4), 74-79.

Johnson, D. W., & Koch, H. (n.d.).

Kanyaru, P., & Kyalo, J. (2015). Factors Affecting the Online Transactions in the Developing Countries: A Case of E-commerce Businesses in Nairobi County, Kenya. *Journal of Educational Policy and Enterepreneurial Research (JEPER), 2*(3), 1-7.

Katua, N. T. (2014). The Role of SMEs in Employment Creation and Economic Growth in Selected Countries. *International Journal of Education and Research, 2*(12), 461-472.

Kimwele, M., Mwangi, W., & Kimani, S. (2013). Adoption of Information Technology Security Policies: Case Study of Kenyan Small and Medium Enterprises (SMES). *Journal of Theoretical and Applied Information Technology*, 47-64.

KIPPRA. (2002). Discussion paper No.20 Review of government Policies for the promotion of Micro and Small-Scale Enterprises. Nairobi, Kenya.

Lokhande, P. S., & Meshram, B. B. (2013). E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. *https://www.researchgate.net/publication/235697382: Retrieved on: 09 March 2016*.

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

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling.* National Institute of Standards and Technology.

Microsoft. (2003, June). *Microsoft*. Retrieved July 20, 2016, from msdn.microsoft.com: https://msdn.microsoft.com/en-us/library/ff648641.aspx

Moftar, A., Abdullah, S., & Hawedi, S. (2012). Challenges of security, protection and trust on E-commerce: A Case of Online Purchasing in Libya. *International Journal of Advanced Research in Computer and Communication Engineering*, *1*(3), 141-145.

Mugenda, O. M., & Mugenda, A. G. (2003). Research Methods. *Nairobi, African Centre for Technology Studies Press*.

Muguchu, M. (2010). *uonbi.* Retrieved 6 22, 2016, from http://chss.uonbi.ac.ke/: http://chss.uonbi.ac.ke/sites/default/files/chss/RELATIONSHIP%20BETWEEN%20ACCESS%20TO%20CREDIT%20AND%20FINANCIAL%20PERFOMAN.pdf

Nabila, A. (2014). *The Impact of Cyber Security on SMEs.* Retrieved May 28, 2016, from utwente.nl: http://essay.utwente.nl/65851/

Ng, Z. X., Ahmad, A., & Maynard, S. (2013). Information Security Management: Factors that Influence Security Investments in SMEs. *Australian Information Security Management*, 60-74.

Ngoma, S. (2012, March 4). Vulnerability of IT Infrastructures: Internal and External Threats. Retrieved from http://www.congovision.com/IT-Security-Pub.pdf

Niranjanamurthy, M., & Chahar, D. (2013). The study of E-commerce Security Issues and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering*.

Nooteboom, B. (1994). Innovation and diffusion in small firms. *Theory and Evidence Small Business Economics, 6*(5), 327-347.

Onwubiko, C., & Lenaghan, A. P. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. *IEEE International Conference on Intelligence and Security Informatics.*

PACIS. (2013). *What increases firms' performance of information security management and the role of regulatory pressure.* Retrieved from http://www.pacis-net.org: http://www.pacis-net.org/file/2013/PACIS2013-100.pdf

Pease, W., & Michelle, R. (2003). *E-commerce and small meium enterprises (SMEs) in reguonal communities.* Retrieved 6 8, 2016, from researchgate.net: https://www.researchgate.net/publication/242161990_E-commerce_and_small_and_medium_eenterprises_SMEs_in_regional_communities

PWC. (2015). 2015 Information Security Breaches Survey.

Rahman, S. (., & Lackey, R. (2013). E-commerce systems security for small businesses. *International Journal of Network Security & Its Applications*.

Riquelme, H. (2002). Commercial Internet Adoption in China: Comparing the experience of large business internet research. *Electronic Networking Applications and Policy, 12*(3), 276-286.

Roberts, M., & Wood, M. (2002). The Strategic Use of Computerised Information Systems. *Micro Enterprise Logistics Information Management, 15*(2), 115-125.

Sawma, V. D., & Probert, R. L. (2003). E-commerce authentication : An effective countermeasures design model.

Schultz. (n.d.). *Firewalls: An Effective Solution for Internet Security - IT Today.* Retrieved May 28, 2016, from www.ittoday.info: http://www.ittoday.info/AIMS/DSM/83-10-40.pdf

Sen, P., Ahmed, A., & Islam, R. (2015). A study on e-commerce security issues and solutions. *International Journal of Computer and Communication System Engineering, 2*(3), 425-430.

Shemi, A. P. (2012). *Factors Affecting E-Commerce Adoption in Small and Medium Enterprises: An Interpretive Study of Botswana.* Phd Thesis, University of Salford.

Singh, J. (2014). Review of e-commerce security challenges. *International Journal of Innovative Research in Computer and Communication Engineering, 2*(2), 2850-2858.

SME FEST. (n.d.). Retrieved May 30, 2016, from The Kenya SME Sector Case Study: http://www.smefest.co.ke/sme-sector/

Sobihah, A., Embat, S., Amin, M., & Muda, M. (2014). Organization, The Relationship between E-Commerce Adoption and Performance. *International Journal of Business and Management, 9*(1), 56-62.

Souter, D., & Kerrets-Makau, M. (2012). *Internet governance in Kenya – an assessment for the internet society.* ICT Development Associates Limited.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce,* 135-161.

Treese, G., & Stewart, C. (1998). *Designing systems for internet commerce.* New York: Addison-Wesley.

Venkatesh, V., & Davis, F. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204.

Vilaseca, J. (2013). *Las TIC y las transformaciones de la empresa catalane. Barcelona.* Foundation for the Open University of Catalonia.

Watuthu, S., Kimwele, M., & Okeyo, G. (2015). The Key Issues Surrounding Electronic Commerce Information Security Management. *International Journal of Soft Computing and Engineering (IJSCE), 5*(1), 37-42.

Xynos, K., Sutherland, I., & Blyth, A. (2013). *Effectiveness of blocking evasions in Intrusion Prevention Systems.* Pontypridd: University of South Wales.

Yanyan, W. (2014). Research on e-commerce security based on risk managment perspective. *International Journal of Security and Its Applications* , 153-162.

Yazdanifard, R., AbuTabik, M. A., & Seyedi, A. P. (2011). Security and Trust in Electronic Commerce - Finding the Safe Side. *International Conference on Information Communication and Management, 16*, 141-146.

APPENDICES

APPENDIX I: INTRODUCTORY LETTER

TO WHOM IT MAY CONCERN.

Dear Sir/Madam,

RE: PERMISSION TO CARRY OUT A RESEARCH ON E-COMMERCE SECURITY THREATS AND ORGANIZATIONAL PERFORMANCE OF (SMEs) IN NAIROBI, KENYA.

I am a bona fide continuing student in the Master of Business Administration degree program at the University of Nairobi. In partial fulfilment of the degree, I am required to carry out a research as aforementioned. The study seeks to identify real management problems and being one of the SMEs in Nairobi, your business is the main focus of the study. Kindly provide assistance by filling of the questionnaire attached here-in. The information requested is needed purely for academic purposes and will be treated as confidential and will not be used for any other purpose apart from my research. It will also be made available to you upon request.

Yours Faithfully,

Eva W. Ngugi

APPENDIX II

QUESTIONNAIRE

INSTRUCTIONS

I am a University of Nairobi, MBA student and this questionnaire seeks to collect information on e-commerce security in Small and Medium Enterprises (SMEs) in Nairobi County, Kenya. Please provide information in the spaces provided and tick in the appropriate boxes. All the information received will only be used for academic purposes.

SECTION A: GENERAL INFORMATION

Individual Data

1. Which of the following best describes your role in the organization?

Senior Management ☐ Middle Management ☐ Junior Management ☐

2. Please indicate your gender

Male ☐ Female ☐

3. Please select the age group that best describes your age (in years).

25or Below ☐ 26-30 ☐ 31-35 ☐ 36- 40 ☐ Over 40 ☐

4. Please indicate your highest level of education

Primary …… ☐

Secondary…….. ☐

University …… ☐

Other (Specify)……..

SME Data

5. What type of enterprise is this business?

   Sole proprietorship…… ☐

   Partnership …… ☐

   Private Limited Company … ☐

   Public Limited Company …. ☐

   Other (Specify…….

6. How many full time employees are employed in this business? _____

7. Age of the Business (in years)

   5 or Below ☐ 6-10 ☐ 11-15 ☐ 16-20 ☐ Over 20 ☐

8. Which category best describes your business?

   Food, Beverage and Tobacco …… ☐

   Books and Stationery……. ☐

   Energy, Electrical and Electronics…… ☐

   Plastics and Rubber…… ☐

   Pharmaceutical and Medical Equipment ….. ☐

   Others (Specify)……

9. How long has the firm been using e-commerce? (in years)

   5 or Below ☐ 6-10 ☐ 11-15 ☐ 16-20 ☐ Over 20 ☐

10. Is the business likely to continue with the use of e-commerce?

    Very Likely ☐ Likely ☐ Unlikely ☐

SECTION B: Types of e-commerce security threats

Indicate the extent to which the organization has faced each of the following e-commerce security threats. Use the scale

[1-No Extent; 2–Small Extent; 3 - Moderate; 4- Large Extent; 5- Very Large Extent]

Kindly select where applicable (use a tick [√])

	Types of Security Threats	**1 (No Extent)**	**2 (Small Extent)**	**3 (Moderate)**	**4 (Large Extent)**	**5 (Very Large Extent)**
1	Malicious code: *(Viruses and Worms)*					
2	Denial of Service (*attempts to flood the server with excessive amount of data such that access is limited even to the legitimate users)*					
3	Social Engineering (*involves smooth talking the user to reveal personal information)*					
4	Procedural penetration (e.g *former employees having the list of valid passwords using them against the company)*					
5	Hackers and attackers (*unauthorized users on the network with malicious intent)*					
6	Unauthorized access *(It may sabotage hardware and manipulation of software)*					
7	Authentication and Privilege attacks (*mostly because of the use of weak passwords and policies)*					
8	Repudiation *(ability of users to deny that they performed specific actions*					
	Other (Specify)					

SECTION C: Security Countermeasures to curb Security Threats

Indicate the extent to which the organization has used each of the following countermeasures to counter e-commerce security threats. Use the scale

[1-No Extent; 2–Small Extent; 3 - Moderate; 4- Large Extent; 5- Very Large Extent]

Kindly select where applicable (use a tick [√])

	Types of Countermeasures	**1 (No Extent)**	**2 (Small Extent)**	**3 (Moderate)**	**4 (Large Extent)**	**5 (Very Large Extent)**
1	Antivirus (*used against viruses)*					
2	Role Separation (*separation of duties to avoid privilege creep)*					
3	Backup and redundant systems (*especially for database and server attacks restoration)*					
5	Security Policies (*management of security in the organization*)					
6	Security Awareness*(to prevent from trust exploitation like social engineering)*					
7	Password policies (*to enforce stronger passwords)*					
8	Update of patches (*to reduce attacks due to out of date patches*)					
9	Firewalls (*prevent from unauthorized access*)					
10	Encryption *(transforms plain text into cipher text thus securing stored information)*					
11	Other (Specify)					

SECTION D: Challenges in managing security threats

Indicate the extent to which the organization faces each of the following challenges in managing e-commerce security threats. Use the scale

[1-No Extent; 2–Small Extent; 3 - Moderate; 4- Large Extent; 5- Very Large Extent]

Kindly select where applicable (use a tick [√])

	Challenges of managing security threats	**1 (No Extent)**	**2 (Small Extent)**	**3 (Moderate)**	**4 (Large Extent)**	**5 (Very Large Extent)**
1	Financial Constraints					
2	Lack of strategic direction					
3	Weak Passwords					
4	Complexities of Security policies					
5	Lack of competent IT personnel					
6	Misconception of e-commerce costs					
7	Emerging Technologies					
8	Users refusal/inability to comply to set guidelines					
9	Unawareness that they are potential targets					
10	Lack of understanding of security as a whole					
11	Other (specify)					

SECTION E: Effect of E-commerce Security in Performance of SMEs

Indicate the extent to which the organization has performed for each of the following organizational performance parameters. Use the scale

[1-No Extent; 2–Small Extent; 3 - Moderate; 4- Large Extent; 5- Very Large Extent]

Kindly select where applicable (use a tick [√])

	Organizational Performance	**1 (No Extent)**	**2 (Small Extent)**	**3 (Moderate)**	**4 (Large Extent)**	**5 (Very Large Extent)**
1	Profitability					
2	Saving Costs					
3	Time saving					
4	Increased Sales					
5	Industry Leadership					
6	Market Value					
7	Overall Business Performance and Success					

THANK YOU FOR TAKING TIME OUT OF YOUR BUSY SCHEDULE TO ANSWERTHIS QUESTIONNAIRE

APPENDIX III

Kenya Top 100 SMEs- 2015

1. ATLAS PLUMBERS AND BUILDERS
2 TROPIKAL BRANDS AFRIKA
3 KEPPEL INVESTMENTS LTD
4 SHIAN TRAVEL
5 RUPRA CONSTRUCTION CO.
6 POWERPOINT SYSTEMS (E.A) LTD
7 CHEMICAL AND SCHOOL SUPPLIES
8 SATGURU TRAVEL AND TOURS
9 RADAR LTD
10 KENTONS LTD
11 AVTECH SYSTEMS LTD
12 SAI PHARMACEUTICALS LTD
13 KUNAL HARDWARE AND STEEL
14 CONINX INDUSTRIES LTD
15 R & R PLASTIC LTD
16 CAPITAL COLOURS C. D LTD
17 ASL CREDIT LTD
18 KANDIA FRESH PRODUCE SUPPLIERS LTD
19 FURNITURE ELEGANCE LTD
20 MURANGA FORWARDERS LTD
21 BBC AUTO SPARES LTD
22 DIGITAL DEN LTD
23 XRX TECHNOLOGIES LTD
24 NAIROBI GARMENTS ENTERPRISE LTD
25 CHARLESTON TRAVEL LTD
26 SPICE WORLD LTD
27 MASTER POWER SYSTEMS LTD
28 SOFTWARE TECHNOLOGIES LTD
29 KENBRO INDUSTRIES LTD
30 SKYLARK CREATIVE PRODUCTS LTD
31 GANATRA PLANT & EQUIPMENT LTD
32 SECURITY WORLD TECHNOLOGY LTD
33 SPECIALIZED ALUMINIUM RENOVATORS LIMITED
34 WINES OF THE WORLD LTD
35 VIRGIN TOURS LTD
36 ARAMEX KENYA LTD
37 CANON ALUMINIUM FAB LTD
38 PANESAR'S KENYA LTD
39 TYRE MASTERS LTD
40 LANTECH AFRICA LTD
41 WARREN ENTERPRISE LTD
42 AFRICA TEA BROKERS LTD
43 MERIDIAN HOLDINGS LTD
44 DUNE PACKAGING LTD
45 THE PHOENIX LTD
46 FAIRVIEW HOTEL LTD
47 SPECICOM TECHNOLOGIES LTD
48 PUNSANI ELECTRICALS & INDUSTRIAL HARDWARE LTD
49 BISELEX (K) LTD
50 VICTORIA FURNITURES LTD
51 GINA DIN CORPORATE COMM

52 AMAR HARDWARE LTD
53 MELVIN MARSH INTERNATIONAL
54 LANOR INTERNATIONAL LTD
55 SYNERMED PHARMACEUTICALS (K) LTD
56 SAHAJANAND ENTERPRISES LTD
57 VEHICLE & EQUIPMENT LEASING LTD
58 SILVERBIRD TRAVELPLUS
59 WAUMINI INSURANCE BROKERS LTD
60 KENAPEN INDUSTRIES LTD
61 HARDWARE AND WELDING SUPPLIES
62 ISOLUTIONS ASSOCIATES
63 MOMBASA CANVAS LTD
64 EAST AFRICA CANVAS CO
65 TOTAL SOLUTIONS LTD
66 PRINT FAST (K) LTD
67 OPTIWARE COMMUNICATIONS LTD
68 DEEPA INDUSTRIES LTD
69 ENDEAVOUR AFRICA LTD
70 TRAVEL SHOPPE CO LTD
71 KEMA (E.A) LTD
72 AMAR DISTRIBUTORS LTD
73 PWANI CELLULAR SERVICES
74 SHEFFIELD STEEL SYTEMS LTD
75 GENERAL ALUMINIUM
76 CREATIVE EDGE LTD
77 BROLLO KENYA LTD
78 TRIDENT PLUMBERS LIMITED
79 PHYSICAL THERAPY SERVICES LTD
80 PRAFUL CHANDRA & BROTHERS LTD
81 DHARAMSHI LAKHAMSHI & CO / Dalco Kenya
82 MADHUPAPER KENYA LTD
83 UNION LOGISTICS LTD
84 OIL SEALS AND BEARING CENTRE LTD
85 SKYLARK CONSTRUCTION LTD
86 BIODEAL LABORATORIES LTD
87 WARREN CONCRETE LTD
88 RONGAI WORKSHOP & TRANSPORT
89 COMPLAST INDUSTRIES LTD
90 KINPASH ENTERPRISES LTD
91 SIGHT AND SOUND COMPUTERS LTD
92 DE RUITER EAST AFRICA LTD
93 ACE AUTOCENTRE LTD
94 KENYA SUITCASE MFG LTD
95 HEBATULLAH BROTHERS LTD
96 MARKET POWER INT. LTD
97 NIVAS LTD
98 SIGMA SUPPLIERS LTD
99 IMPALA GLASS INDUSTRIES LTD
100 EGGEN JOINEX LTD

Source: ***KPMG East Africa and the Nation Media Group***