UNIVERSITY OF NAIROBI

SCHOOL
OF
COMPUTING AND INFORMATICS

The Effects of Cyber-crime on E-commerce; a model for SMEs in Kenya

Submitted by:

WEKUNDAH RUTH NANGECHE – P56/72806/2012

August 2015

Supervisor: DR. Christopher Chepken

Submitted in partial fulfillment of the requirement for the degree of Master of Science in Information systems

Declaration

I Ruth Wekundah confirm that this research project and work presented, it's my own achievement. To the best of my knowledge, this has not been carried out before or previously to other education institution in the world of similar purpose or forum.

Sign______________________ Date _____________________

Name_____________________ Reg. No.__________________

This research project has been submitted for examination with my approval as the University of Nairobi

Supervisor.

Name: **Dr. Christopher Chepken**

School of Computing and Informatics

University of Nairobi - Chiromo Campus

Sign_______________________________

Acknowledgement

I would like to take this opportunity and thank my supervisor who has seen me through the entire journey during the study. Your perspective, insight, experiences and support helped illuminate the complex areas that were not clearly understood, hence mystifying the intricate interplays.

I also would like to thank the panel committee who were helpful in giving variant ideas and comment brought forth in my presentation. Your input was valuable in the entire project life cycle.

I would like to thank my husband for the encouragement and understanding he gave me in the entire period, an anchor of support for hard work and determination.

Thank you God would not have come this far if it were not for your mercies to ensure that I have good health and energy to move on to completion.

Table of Contents

List of Figures

List of Tables

Abstract:

Technology has become the norm of various activities within our business. Its ubiquitous state has seen businesses adapting to innovative products and services to its customers, developing customer centric strategies in order to deliver customer friendly products and services to the target market. Since technology itself has become indispensable with it comes a tunnel of attack which affects the confidentiality, integrity and availability of information in businesses.

Most assets for SMEs are usually vulnerable to cyber-attacks due to their business model hence unable to put in place structures to minimize or mitigate against attacks to their assets. SMEs fall victims of these attacks and this has resulted to either massive loss of businesses or closure of some SMEs. It is evident from this study that there is need to treat SMEs different in terms of cybercrime security from large pool of corporates. When Cybercrime attacks occur, organizations need to assess the damage and loss from this crime. While large organizations have the mechanisms to determine such losses, SMEs lack such capability and often ignore the need to implement effective information security measures.

This study focusses on the various cyber-attacks that SMEs fall victims of. Further analysis was done on the various cybercrime models that are used by organization to counter cyber-attack. Most of the existing cybercrime models are reactive after a cyber-attack has been committed and are not specific on SMEs. Both qualitative and quantitative research methods were used in this study to collect data from various SMEs on cyber-crime attack. From the findings, it was very clear that most SMEs do not put emphasis or assign enough resources on cybercrime attack and yet fall victims of continuous attacks. The SMEs have minimal, or no expertise, to tackle cyber-crime and rely heavily on friends or the internet for cyber-attack information. Input from the existing models, secondary sources and collected data has enabled realization of the cybercrime model for SMEs which focusses on preventive, detective and reactive measures in the fight against cybercrime. There is also focus on the government and how they can come in strongly and support SMEs especially with use of the CERT systems in place, depending on the SMEs nature they can get advice and support in an event of a cyber-attack. This will enable SMEs reduce on their manpower and rely on the arm of the government for advise and support on Cybercrime activities.

Definition of Terms:

SME: Small and Medium Enterprises based on the number of employees, SMEs is defined as those enterprises below a certain predefined number of workers (i.e. can range from less than 10 to less than 100 employees) Jaques, R. (2003).

Cybercrime violence: This involves stalking, hate-speech via online such as the social mediums Ciardhuáin, S. (2004)

Cybercrime trespass: Emphasis is on hacking which ranges from ethical hacking to information warfare Ciardhuáin, S. (2004)

Cybercrime theft: Fraud; appropriation of intellectual property Ciardhuáin, S. (2004)

Denial of Service Attacks (DoS): Denial of service attack, one unable to utilize his computer to its full potential, Jaishankar, K (2009):

Asset: Anything that has potential value to the business is an asset. This might be fixed assets such as building, monetary or even skills within the organization O'hanley, R. (2013)

Vulnerability: Weakness in an asset that can be exploited by a threat Suter, M (2007)

Threat: This is an attack to an asset, making it not achieve its full potential to the business. Casey, E. (2000).

CERT: Computer Emergency Response Teams, Kyobe, M. (2008

Zombie computers: One unable to make maximize use of their computers or machine due to interference or denial of service attacks Jaishankar, K (2009):

E-commerce: Stands for electronic commerce which deals with the facilitation of transactions and selling of products and services online, that is, via the internet or any other telecommunications network, L.M. Smith. (2008)

CHAPTER ONE

1.0 INTRODUCTION AND BACKGROUND

1.1 Introduction

Technology is used in so many ways and its increasingly becoming the norm of all activities. Industries and companies use internet for communication, billing account management, good distribution and ecommerce.

Internet was developed for better communication and research with advancement of technology and expansion of internet every area becomes easy to access but it also provides a pathway to commit crimes easily without any effort only system knowledge Kansal (2014).

Beal (2010), defines Cybercrime as that which encompasses any criminal act dealing with computers and networks (called hacking). Additionally, Cybercrime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be Cybercrimes when the illegal activities are committed through the use of a computer and the Internet.

Cybercrime is “unlawful acts wherein the computer is either a tool or target or both”. The may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. Asma (2013).

Moore (2005) defines Cybercrime as Investigating High-Technology Computer Crime where Cyberspace criminals interfere with the day to day technology operations in a company.

According to Marjie (2013) the marriage of telecommunication and computer has yield to Cybercrime due to the web and its promise of anonymity.

Marjie (2013) categories online crime as follows;

i. Interference with lawful use of computers: **DOS attacks, viruses, worms, other malware, cyber vandalism, cyber terrorism, spam, etc.**

ii. Theft of information and copyright infringement: **Industrial espionage, identity theft, identity fraud**

iii. Dissemination of contraband or offensive materials: **Online gambling, treasonous or racist material**

iv. Threatening communications: **Extortion, cyberstalking, cyber harassment, cyberbullying,**

v. Fraud: **Auction fraud, credit card fraud, theft of services, stock manipulation**

E-commerce stands for electronic commerce which deals with the facilitation of transactions and selling of products and services online, that is, via the internet or any other telecommunications network (Jelassi & Enders, 2008). This involves the electronic trading of physical and digital goods, quite often encompassing all the trading steps such as online marketing, online ordering, e-payment for digital goods, online distribution and after-sales support activities.

SMEs go through different stages in adopting e-commerce. They start with creating a Web site primarily to advertise and promote the company and its products and services. When these firms begin generating traffic, inquiries and, eventually, sales through their Web sites, they are likely to engage in e-commerce. We have various sectors for SMEs practicing E-commerce in Kenya, such as the agricultural sector, tourism, and supply chain functionalities.

E-commerce involves much more than electronically mediated financial transactions between organizations and customers. This can either be through emails to maintain a business relationship with other companies (electronically mediated transactions) between the company and third party (Chaffey, 2009).

A recent survey by MasterCard on online shopping in Kenya indicated that out of the 86% of Kenyans who do not shop online, 38% raised their concerns about the time it would take to get items delivered to them while an additional 38% were not sure that making transactions online was secure.

According to Kenya cyber security report 2014, Kenya loses 2 billion annually on Cybercrime. In the year 2013, Cybercrime attacks grew by 108% (5.4million attacks) from previous year 2012 (2.6million attacks). Kenya's a soft target as 85% of all web applications in the country are insecure thus available for attacks.

The Cybercrime attacks are bound to grow as internet penetration is vastly engrossed in Kenya. Despite all these challenges, the e-commerce in Kenya is growing at a percentage of 19 %. This is according to a research done by Synovate Group in 2014.

These risks can be minimized by establishing effective controls. In addition, Web assurance services can be used to provide various levels of assurances that controls are in place (Runyan et al. 2008).

SMEs represent a pillar in our social and economic structures in Kenya, without having mechanisms in place to prevent Cybercrime might lead to decline of growth of our economy. According to Charmayne Cullom, (2001) Enforcement put in place for Cybercrime ensures that SMEs are able to avoid cyber threats which might not only cause losses in their businesses but also cause closure of their businesses.

Some initiatives that some online firms are doing to ensure that it's safe for customers to input data that is sensitive by use of a virtual pin pad on screen thus avoiding keyboard strokes that can be captured by malicious software on the computer. This becomes a challenge especially when customer is not within the vicinity and are using a personal / connectivity to their websites.

Encryption is also key, in that businesses are opting to have security digital servers to ensure that communication between them and their customers is secured and cannot be deciphered. Most of the multinational corporates have enforced this but not SMEs.

Government should be on the fore front to ensure that it the relevant regulations are in place for Cybercrime and also that it encourages the masses to embrace e-commerce.

In July last year, 2014 Kenya (TESPOK) Telecommunication service provider of Kenya and other cyber security teams from all over the world, analyzed the role of the private sector in dealing with Cybercrime, here they came up with some recommendation which the government was to come up with a comprehensive Cybercrime law to deal with the cyber criminals. The government came up with a Cybercrime and computer related bill but which has been criticized by some that it falls below international standards and for the content it lacks privacy and freedom of expressions.

Most SMEs do not comply with the existing Information security management standards such as the ISO 27001.The standards have provision to assist the SMEs have a robust information security framework to guard against Cybercrime attacks.

The proponents of situational crime prevention theory argue that it is necessary to forestall the crime from occurring in the first place, as opposed to concerning themselves with detecting the crime or punishing the criminal after the crime has occurred Clarke (1997).

1.1 Problem Statement

SMEs are the pillars of our economic and social growth in Kenya. Most SMEs fall victims of Cybercrime attack due to their business model Clarke (1997). We find that due to their nature, SMEs usually minimize their Information technology costs to a point that they outsource their technology services, they are heavy on Cloud services and sometimes some employees' face the BYOD (Bring Your Own Device) at work to cut down costs on technology equipment and this causes their vulnerability to viruses, worms at their places of work.

According to Beal (2010) SMEs fall victims of Cybercrime attacks as most of them have links with the large enterprises or organization, hence used as a tunnel to attack the big enterprises. Beal (2010) describes further on SMEs stating that with their cost cutting nature they easily fall victims of denial of service where their server might be compromised or pay heavy when recovering from attacks as most of them do not have measures in place for contingency planning. Their low cutting budget causes them to be victims of software piracy and trade and logo attacks as they might not be able to sniff out illegal use of their trademarks in the internet. Beal (2010

SMEs usually have fewer resources and expertise in strategic and operational IT security policies and task in comparison to the large organization. Clarke (1997).

Most of the SMEs have very few employees who might not be well versed with issues relating to IT security or any of the IT security standards. Charmayne Cullom, (2001)

1.2 Research Objectives

1.2.1 Overall Objective;

i. To develop a model for SMEs to be used in combating Cybercrime.

1.2.2 Other Objectives;

i. To establish the seriousness of SME Cybercrime.
ii. To find out the strengths and weaknesses of these measures.
iii. To validate the cybercrime model.

1.3 Research Questions

i. What business processes are they engaged in?
ii. What are the variant cyber-attack crimes that the SME has fallen victim of?
iii. What cyber security measures have been put in place if any?
iv. Any challenge with the security policies and processes they have?

1.4 Justification and significance of the study

This study has enabled SMEs especially those with an online presence to have a seamless way of countering Cybercrime attacks in their businesses. SMEs will now be able to be proactive in the fight against Cybercrime instead of reacting to the variant Cybercrime attacks.

Most studies on Cybercrime usually focus on large corporates; enterprises without any emphasis on the SMEs, this study has focused on SMEs, providing a model that they can use in their fight against Cybercrime.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

Cybercrimes are crimes committed on the Cyberspace using computer and networking technology provided by Information and Communication infrastructures. Chawki, (2009) Observable trends have shown that law enforcement has not been able to scale-up to meet up with the new challenges posed by Cybercrime to the well-being of various categories of users on the Internet (Brenner, 2007). According to Jaishankar, (2009) Cybercrime is now beyond any boundary and countries that have inadequate or no laws around cyber criminals are increasingly becoming very vulnerable to attack.

The following list provides some important definitions (UN-ESCAP, UN-APCICT, and Ministry of Strategy and Finance, Republic of Korea, 2008):

- Cyber vulnerability is susceptibility in the protection of an asset from cyber threats.
- Cyber risks are the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.
- Cyber-threats are potential cyber events that may cause unwanted outcomes, resulting in harm to a system or organization. Threats may originate externally or internally and may originate from individuals or organizations.
- Cyberattacks are the use of malicious codes that may affect computers and networks, and lead to Cybercrime, such as information and identity theft.
- Cybersecurity encompasses all the necessary elements required to defend and respond to Cyber-threats in Cyberspace (e.g., technology, tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, and assurance, among others).
- Cyber resilience is the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recover

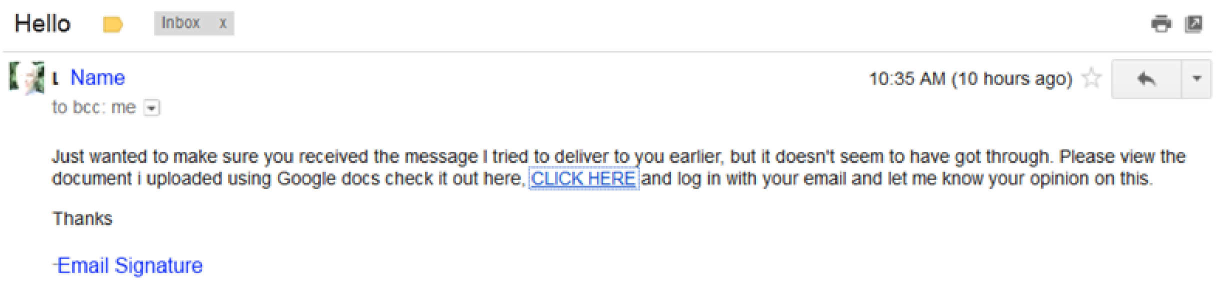
2.2 Common Cyber Attacks

There are many different types of cyber-attacks. Most of these attacks emerge from the network connection that one has to the internet. O'hanley, (2013) we have various forms of attacks that E-business are vulnerable to;

2.2.1 Phishing Attacks

Cyber criminals have been known to set up a replica website to a genuine that is used to collect information from the users of the sites, Phishing Scam is a fraudulent web page, an email, or a text message that attracts the unsuspecting users to reveal sensitive information such as passwords, financial details, or other private data.

Cyber criminals in the past have been able to collect personal information from the online users by providing a replica page that is pushed to online customers and captures their personal information. This is known as phishing and details can be captured directly or an email might be sent to users telling them about the expiry of their credit cards. See sample; (UN-ESCAP, UNAPCICT, 2008):



Hello Inbox x

Name

to bcc: me

10:35 AM (10 hours ago)

Just wanted to make sure you received the message I tried to deliver to you earlier, but it doesn't seem to have got through. Please view the document i uploaded using Google docs check it out here, CLICK HERE and log in with your email and let me know your opinion on this.

Thanks

-Email Signature

Figure 1:Phishing Email Marjie, T. (2013)

Same details captured for the owner of the address and yet they are not the originators for the email.

2.2.2 Man in the Middle Attacks

This attack attempts to insert the attacker in the middle of a communication for purposes of intercepting a client’s data and modifying them before discarding them or sending them out to the real destination.

O’hanley, (2013) describes the two main forms of the man in the middle attack exist:

- Eavesdropping attacks; Getting access to information on the network via radio waves
  Sniffing Attacks
- Manipulation attack; One is able to retransmit data after changing it.
  Spoofing Attacks e.g. Mac address spoofing, IP or frame spoofing.

2.2.3 Denial of Service Attacks

Denial of service (DoS) attacks aim at denying or degrading the quality of a legitimate user’s access to a service or network resource. It also can bring down the server offering such services itself. DoS attacks can be classified into two categories:

The disabling services attack and resource undermining

According to different reports including the annual UNESCAP report on computer crime and O’hanley (2013) the DDoS attacks have induced large financial costs to companies in recent years. In addition, they cause damage to consumer confidence in e-commerce of impacted organizations.

There are various types of DDoS attacks. They all share the same typical structure that is depicted in the below figure. The attacker, in a DDoS, first gains control of several master computers connected to the wireless network by hacking into them, for example. Then the master computers gain control of more computers (zombies) by different means. Finally, a message is sent by the attacker to synchronize all zombies to send the required traffic to the victim. The DDoS is described as in figure 2.

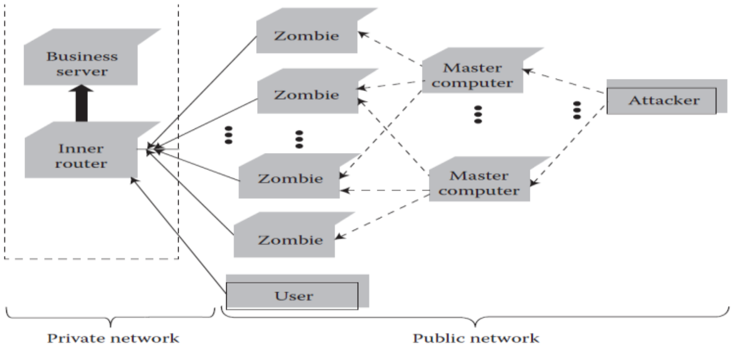


Figure 2: Diagram by O'hanley, (2013) describing the Distributed Denial of service Cyber-attack

2.2.4 Malware Attacks

Malware attacks are malicious software or programs that hinder normal computer operations. Onhanley, (2013) and Rogers, M. and Kathryn C. (2012) defines the various forms of malware or malicious software attacks that are common as per below;

Worms: A worm is a program that makes copies of itself (by various means including copying itself using email or another transport mechanism).

Viruses: A virus is a sequence of code that is inserted into another executable code, so that when the regular program is run, the viral code is also executed.

Trojan: A Trojan is a malware that performs unauthorized, often malicious, actions. The main difference between a Trojan and a virus is the inability to replicate itself.

2.3 Cyber Security Cycle

Due to the extension of potential harm across time, any cybersecurity strategy must be grounded on the cybersecurity cycle, which includes the following three stages in figure 3. (UN-ESCAP, UNAPCICT, 2008):

2.3.1 Preparedness and prevention:

This involves preparing human users and machines to protect themselves against any cyber threat, while promoting security and the avoidance of particularly vulnerable technologies.

2.3.2 Detection: This refers to identifying threats as quickly as possible.

2.3.3 Reaction: This relates to recognizing and correcting the causes of a disruption

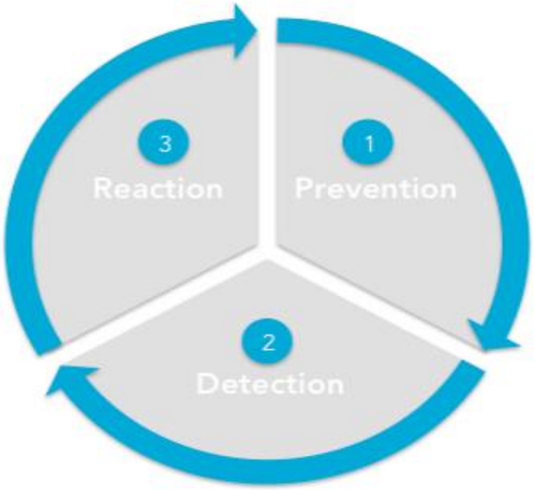


Figure 3: Cyber security cycle (Zaballos, A. and Herranz, F. (2013)

This is able to focus on Cybercrime in a holistic manner. Putting all the aspects in focus for Cyber crime

2.4 Cyber Attack Businesses in Kenya

Small and medium enterprises have become the top target for cyber criminals who steal data, show an Internet security report by Symantec Corporation. The report covering security of institutions 'microfinance, account information, customer data and intellectual property, ranks Kenya at number eight in Africa in terms of threat, a reflection of the wide usage of the Internet by companies.

The global Internet security report indicates that the number of attacks on SMEs grew three-time in the year 2014 to December and represented a 31 per cent of the 69 million attacks in the 157 countries covered by the survey including Kenya.

In Kenya, the report indicates that the country only improved slightly moving to 86 position globally from the previous 85 in terms of security threat level.

In Kenya, we have some businesses that have been attacked by cyber criminals, less has been said or done when businesses are attacked. According to a report by Synovate, Kenya has faced major attacks in the last two years, such as the cyber-attack on Central bank of Kenya in 2013 and Facebook Kenyan 5000 accounts attack by cyber criminals and the NIC bank attack that saw one of the staff being prosecuted for stealing more than 2.8M Kenyan shillings. We have some

SMEs businesses that were attacked and made public such as the radio station, Hope FM which was hijacked by cyber-criminal this year January 2015 for some hours. Most of these attacks are not made public due to the fact that businesses may lose their credibility to their target customers. Some of them might not even know that they were attacked unless financial aspect of it is felt by the business. Most businesses opt to keep silent and recover from cyber-attacks so as not to lose customers.

According to a report by Forbes (2014), data breaches are increasingly becoming the day to day norm especially for companies that have a business to consumer model. In the year 2014, some of the companies that were breached included;

2.4.1 EBAY

EBAY was hacked and the hackers managed to steal 233 million personal records of users including details such as passwords, usernames, phone numbers and physical address compromised. Hackers were able to get access to EBAY credentials thus making EBAY users vulnerable to identity theft.

2.4.2 Domino Pizza

This was hacked by a group called Rex Mundi holding Domino’s Pizza to ransom over 600,000 Belgian and French customer records. In exchange for the personal data, which included names, addresses, emails, phone numbers and even favorite pizza toppings, Mundi demanded $40,000 from the fast-food chain. If the ransom wasn’t met, the hackers threatened to publish the information online.

2.4.3 Sony Pictures

Sony pictures entertainment The Sony Pictures Entertainment hack was a release of confidential data belonging to Sony Pictures Entertainment on November 24, 2014. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers called themselves the "Guardians of Peace" or "GOP" and demanded the cancellation of the planned release of the film *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-un.

2.5 Common Cybercrime for SMEs

2.5.1 Theft and Fraud

This might be physical theft to a computer or any processing equipment beneficial for technical processing. Theft also involves stealing of information which is crucial for the business. Fraud involves credit card offers on online markets to capture personal information where cyber criminals get access to personal information such as credit card information, security card details thus causing fraudulent financial transactions on personal accounts.

2.5.2 Copyright infringement and Phishing

Most SMEs consider purchase of licensed software as costly to their businesses thus ending up using unlicensed software as a cost cutting factor. Charmayne Cullom, (2001) emphasis on variant forms of copyright infringement in SMEs here he focuses on the use of software, programs which is not appropriately purchased and also looks at copy infringement in trademarks and logos of corporation where logos and trademarks of incorporations are posted on websites. Some criminals utilize these logos to appear as legitimate sites for fraud perpetration

Many corporations have employees or consulting contractors who constantly crawl the web to sniff out illegal usage of trademarks and logos. Charmayne (2001) emphasis on Cybercrime focusses on organizations and individuals.

2.5.3 Denial of service

Attacks on organizational information systems may be either physical or logical. There are several instances of web sites, products, and individuals being libeled or attacked by individuals or groups. Denial of Service Attacks (DoS) target specific web sites and associated servers. Some of the newsworthy examples of DoS during 2000 - 2001 have occurred at Microsoft.com, eBay.com, and Amazon.com.

2.6 Cybercrime Continuous Attack on SMEs

2.6.1 Lack of awareness and knowledge of being a Cybercrime victim

Baker (2010) argues that the process of collection and analysis of Cybercrime data is often affected by a lack of understanding of what Cybercrime means or represents. This causes small businesses to continue to be victims of Cybercrime as they are not aware or its characteristics, recognition and measurement in an event that they are attacked.

According to Jacque, (2003) SME managers are reported to be insensitive to Cybercrime as they are considered to make decisions without considering on their vulnerability and also that they are likely to be victims of subsequent attacks on Cybercrime.

This is rampant especially for SMEs as they may not set aside funds to cater for Cybercrime and may not have security awareness and trainings for their employees especially those dealing with the online interactions.

2.6.2 Risk Management skills

The goal of risk management is to identify measure, control and minimize losses associated with uncertain events (Patel and Zaveri, 2010). Most SMEs do not conduct risk management process in their companies, hence there is no assessment done that can help them identify their weak point and mitigate against this. Risk analysis is perceived by SMEs as being complex, requiring specialist expertise and therefore something to be outsourced (Dimopouloulous et al, (2003) thus they may need a third party for any assessment and it is usually a difficult task for the SMEs to decipher points of vulnerability in their businesses.

2.6.3 Information system security infrastructure

The design of the security system may also impact on the recognition and estimation of losses. Modern business environment comprises of many different applications and systems and each of these has its own threat profile (Conklin and Dietrich, 2008). This is usually a challenge as SMEs security practitioner are not able to come up with a comprehensive report on security due to the infrastructure being put together in piecemeal security schemes.

The SMEs may also not put up the security schemes or enforce what is in existence due to their small nature and their lack of awareness on the different kinds of attacks that they are vulnerable to. Most SMEs usually do not possess security and compliance policies (Kyobe, 2008), and a few engage in formal planning thus making most SMEs unable to handle security issues before hand.

2.6.4 Attitude to information Security by the management

According to Kyobe, (2008) Proactive-risk handling is defined as the process in which potential risks to a business are identified in advance, analyzed, mitigated and prevented, and the cost of protection balanced with the cost of exposure to the risk. This does not appear to be done by small business managers or entrepreneurs. For instance, many entrepreneurs are reported to have started businesses without giving proper consideration to economic, environmental, and cognitive limitations (Orford et al, 2004.

Nattaradol (2002) also shows that lack of pro-activeness and proper evaluation of ICT projects resulted in misjudgment or under-estimation of potential business and security risks. He identified several practices in ICT adoption which are indicative of irrational planning or behaviors (e.g., failure to estimate project costs, use of unskilled or untrained staff to manage ICT installations, use of obsolete hardware and software and ignoring potential impact of hackers and sneakers). In addition, small business managers tend to have a strong desire for autonomy

2.6 Regulations on Cybercrime

Security policies ensures that companies proactively identify Cybercrime attack and seek ways in which this can be stopped from occurring

2.7 Good Practices to Mitigate Cyber Crime

According to the United Nations report on Cybercrime 2013, In order to be able to prevent Cybercrime, one needs to have strategies in place and measures that seek to reduce risk of crime occurring. Countries highlight that good practices on Cybercrime prevention include:

i. Law enforcement on the investigation, prosecution of Cybercrime offense putting into consideration handling of electronic evidence.
ii. Effective leadership taking security with top most priority in businesses.
iii. Education and awareness: The development of a strong knowledge base and training on the various forms of Cybercrime.
iv. Cooperation across government, communities, private sector and internationally to act as a global response and profiling of some Cyber-criminals.

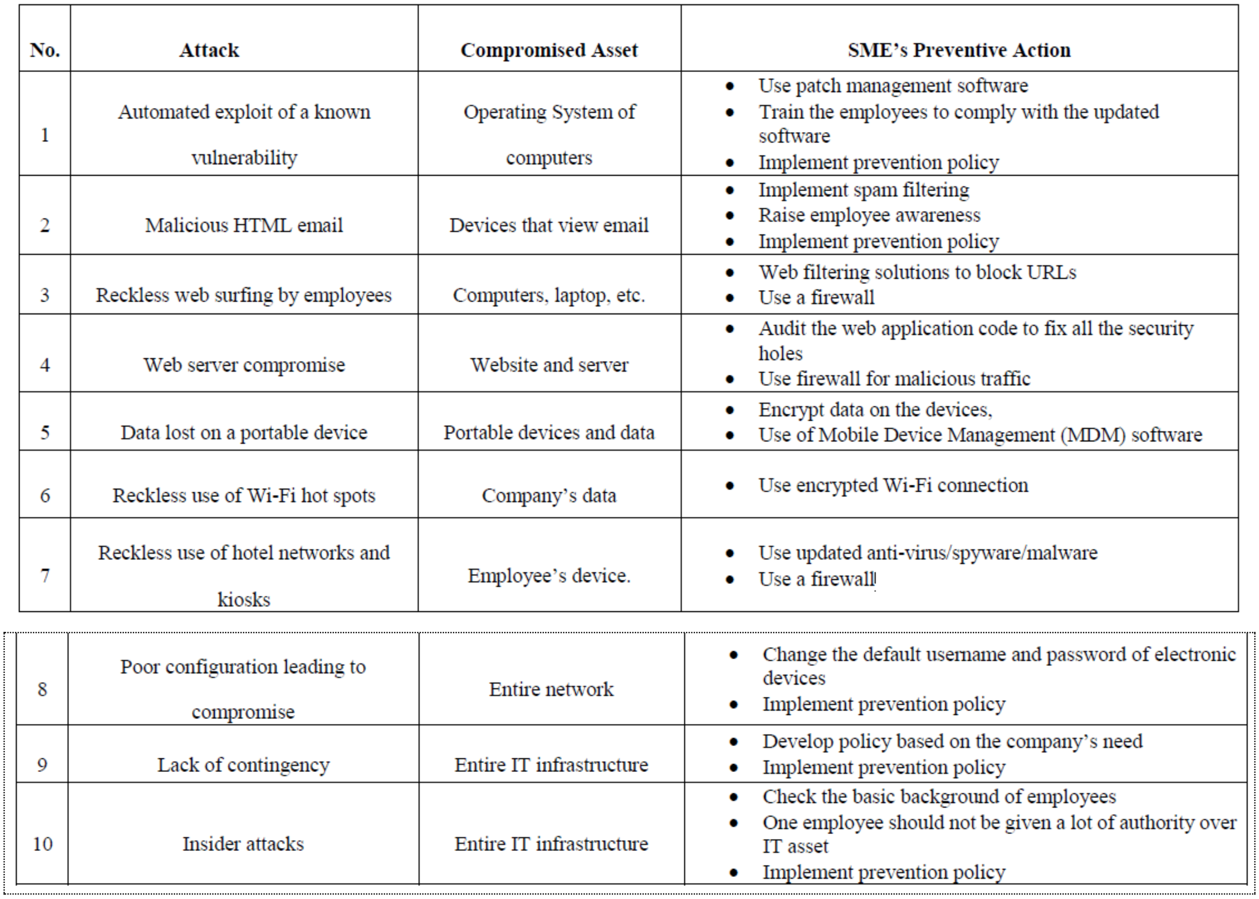
v. Technical structures; Software and hardware in place to mitigate any attacks on Cybercrime.

More than one half of countries report the existence of Cybercrime strategies. In many cases, Cybercrime strategies are closely integrated in cybersecurity strategies. Around 70 per cent of all countries reported national strategies included components on awareness raising, international cooperation, and law enforcement capacity. For the purposes of coordination, law enforcement and prosecution agencies are most frequently reported as lead Cybercrime institutions.

2.7.1 SMEs Cyber Attack and Prevention Actions

Conklin, W. A., and Dietrich, G. (2008, January 7 describes the different attacks for SMEs Cyber-attacks and prevention actions as per table 1 below;

Table 1: Conklin, W. A., and Dietrich, G. (2008) SMEs Cyber-attacks and prevention



No.	Attack	Compromised Asset	SME's Preventive Action
1	Automated exploit of a known vulnerability	Operating System of computers	• Use patch management software • Train the employees to comply with the updated software • Implement prevention policy
2	Malicious HTML email	Devices that view email	• Implement spam filtering • Raise employee awareness • Implement prevention policy
3	Reckless web surfing by employees	Computers, laptop, etc.	• Web filtering solutions to block URLs • Use a firewall
4	Web server compromise	Website and server	• Audit the web application code to fix all the security holes • Use firewall for malicious traffic
5	Data lost on a portable device	Portable devices and data	• Encrypt data on the devices, • Use of Mobile Device Management (MDM) software
6	Reckless use of Wi-Fi hot spots	Company's data	• Use encrypted Wi-Fi connection
7	Reckless use of hotel networks and kiosks	Employee's device.	• Use updated anti-virus/spyware/malware • Use a firewall
8	Poor configuration leading to compromise	Entire network	• Change the default username and password of electronic devices • Implement prevention policy
9	Lack of contingency	Entire IT infrastructure	• Develop policy based on the company's need • Implement prevention policy
10	Insider attacks	Entire IT infrastructure	• Check the basic background of employees • One employee should not be given a lot of authority over IT asset • Implement prevention policy

2.8 Cybercrime Models

Ciardhuáin, S. (2004) defines the importance of Cybercrime models in various aspects. Cybercrime models can act as a point of reference framework especially when looking at activities around Cybercrime. It is a common area or ground that once can discuss on technology share or exchange expertise to proactively identify opportunities for future deployment of technology in various organization.

In order for the models to be comprehensive, they should be able to incorporate all aspects comprehensively.

2.8.1 Conventional Model

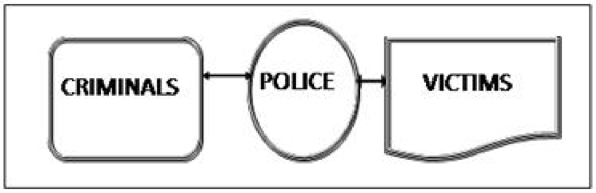


Figure 4: Community Policing Peel Model, Rob Peel, (1829)

i. The model focused on law enforcement after a crime has happened.

ii. Rob Peel, (1829) few or no emphasis on the citizens, as they are the main victims yet have very minimal responsibility.

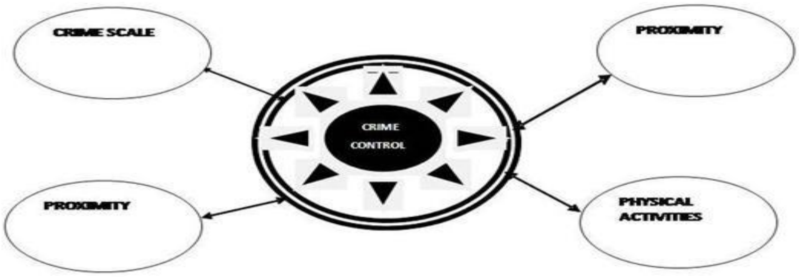


Figure 5: Real world Crime Characteristics, Longe et al, (2010)

i. Proximity of Victims and Offenders.

ii. Magnitude of Crime focusses on number of criminals and victims.

iii. Environment, limitation that causes the crime to occur or not to.

iv. Crime trends to profile and track them down in accordance to trend.

2.9 Cybercrime Challenge

A major challenge that Cybercrime poses to the Peel Model is the ability to react to automated crime Longe et al, (2010). This is because Cybercrime does not share some of the characteristics of conventional crimes that shaped the current Peel model of law enforcement.

i. No proximity is required between victims and violators.
ii. Cybercrime are faceless crimes unless the criminal chose to meet the victims as is the case with fraudulent cyber transactions.
iii. The criminal(s) can commit crimes against individual or individuals in multiple of places at the same time therefore there is multiple victimization from multiple locations or from a single location.
    a) These criminal(s) use computers and other resources in cyber space systems belonging to other unsuspecting users as bots, zombies or detours without their knowledge. They therefore criminalize their victims.

2.9.1 Real Time Response Cyber Crime Model [Longe et al, (2010)]

This is a real time interactive model that aids in identification, location, reporting and apprehension of Cybercrime criminals. Longe et al, (2010) this model focuses on the fact that Cybercrime is committed on the Cyberspace and the criminal might not be in close proximity with the victims. The model figure 6 shown below provides valves that assist users identify malicious intentions through a multi-level access control mechanism.

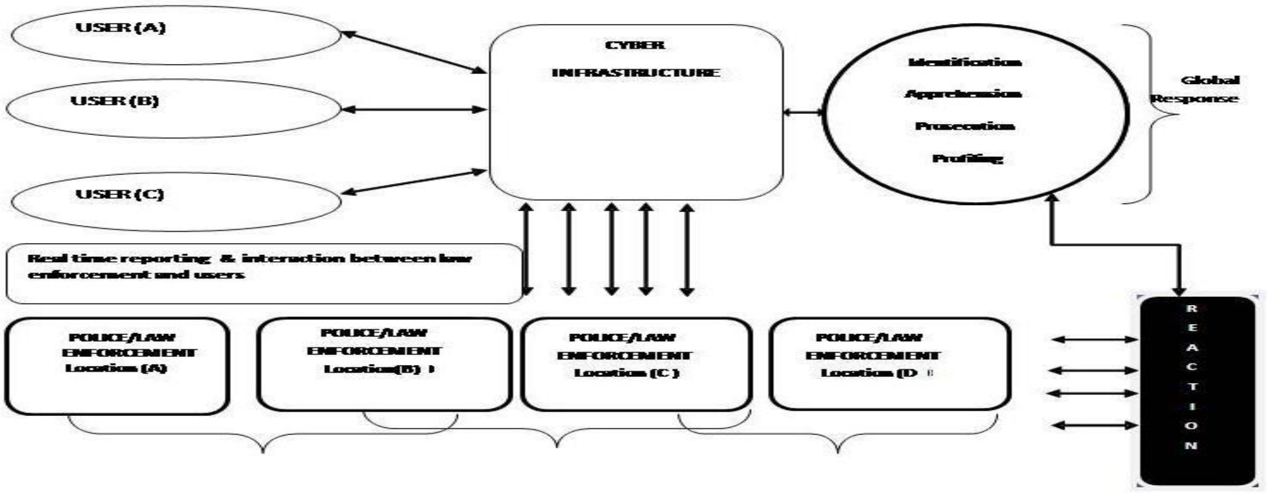

USER (A)
USER (B)
USER (C)
CYBER INFRASTRUCTURE
Identification
Apprehension
Prosecution
Profiling
Global Response
Real time reporting & interaction between law enforcement and users
POLICE/LAW ENFORCEMENT Location (A)
POLICE/LAW ENFORCEMENT Location(B)
POLICE/LAW ENFORCEMENT Location (C)
POLICE/LAW ENFORCEMENT Location (D
REACTION

Figure 6: Real time response model (Longe et al, 2010)

2.9.2 Lee's Model of Scientific Crime Scene Investigation

Lee et al. (2001) discuss Cybercrime scene investigation as a process. This model deals only with crime scene investigation, not with the full process. It identifies four steps within the process.

Recognition**:** The investigator looks at items of potential evidence, the findings have to be documented and preserved.

Identification**:** Evidence collected, has to be classified and compared to the existing properties of evidence such as physical or biological.

Individualization: Uniqueness of the evidence collected is linked to an event or a person through evaluation and interpretation.

Reconstruction**:** focuses on a detailed account of the investigation on the actions and events. This activity leads to reporting and presentation.

Lee et al model limitation

- The model emphasizes on a systematic and methodological way of dealing with Cybercrime which might not always be the case on cyber.

- This model focusses on the physical evidence of collecting evidence, this is not always the case on Cybercrimes.
- Exchange of information with other investigators are not addressed in the model.

2.9.3 Casey

Casey, (2000) came up with a model on Cybercrime that focused on the processing and examination of Cybercrime digital evidence.

Recognition, Preservation, collection, and documentation Classification, comparison, and individualization and finally ends with Reconstruction.

Casey lays emphasis on classification; comparison and individualization as this are the steps where evidence is analyzed. For Casey, (2000) the whole process is a cycle and can begin again under reconstruction.

Here the computer is analyzed first followed by the network layer top to the application layer.

Drawbacks

- The model lays emphasis on the investigation process this is after the crime has occurred.
- The model is too general and not specific to a particular target group in this case SMEs.

2.9.4 Reith, Carr and Gunsch

Reith, Carr and Gunsch (2002) came up with a model that was derived from Digital Forensic Research workshop. This model concentrates on some key activities that were focused on the digital research workshop. Identification, Preparation, Approach strategy, Preservation, Collection, Examination Analysis, Presentation, Returning Evidence. Model can fit in any technological setting but not specific to a particular target group.

This model can act as a reference point for development of techniques that can be used to enquire or investigate thoroughly on the crime but major drawback is that it lays emphasis on the investigation process after a Cybercrime has occurred.

Table 2: Summary of the existing Cybercrime models, depicting model dimension and inventor

MODEL NAME	DIMENSION	Inventor
Peel Model	• Conventional crime scene • Little emphasis on Cyber space	Rob Peel (1998)
Real time response Model	• It takes in to consideration that the crime is committed in the cyber space • Focusses on identification and apprehension of cyber criminals • Offers variant valves to curb cyber criminals • The model has much emphasis on large organization.	Longe O.B., Mbarika V.W., Jones .C. , Anadi .A., Wada (2010)
LEE'S MODEL	• Focusses on systematic methodological way on Cybercrime, this is not always the case • Lays emphasis on physical evidence, this is not always the case on cyber • Exchange of information with other investigator not addressed in the model.	Lee, H. C., Palmbach, T. M., & Miller, M. T, (2001)
Casey Model	• Focus on processing, examination of digital evidence • Emphasis on individualization steps of evidence analysis • This model caters for Cybercrime after crime has occurred • The model is too general not specific to target group	Casey. E, (2000).
Abstract model of computer forensic process	• Driven by digital forensic research workshop • Lays emphasis on key activities after a Cybercrime has taken place • Model can fit on any technological setting but not targeted to a specific group.	**Reith, Carr and Gunsch, (2002)**

2.9.5 Conceptual Model

We have quite a number of models that exist on Cybercrime. Most of the models do lay emphasis on the activities to do after the crime has been committed and the processing of the digital evidence. The model should be comprehensive to a point that it can support development of new tools, new techniques and training that can be accredited and that there is a way in which information flows for best practices. The model should be able to take into consideration the target group that the framework will be applicable and ensure that it suits this target group.

Suter, (2007) for any protection of information in an organization to flow flawless, there has to be some form of control.

Input of the proposed Conceptual Model**:**

- Existing models on Cybercrime.
- Reports, reference and Cybercrime strategies.
- SMEs structures and their business setting.

The conceptual model as depicted in figure 7 was used in the development of the final model for SMEs.

Table 3: Cybercrime Conceptual Model References

Component	Description	Source
▪ **Prevention and Early warnings** ▪ **Detection** ▪ **Reaction** ▪ **Crisis Management**	• Preparedness of Humans and machines against Cybercrime attacks. Avoidance of vulnerable decisions or technology. • Identification of threats as quickly as possible • Recognize and correct the cause of disruption • Plan in place with roles and responsibilities	• (UN-ESCAP, UNAPCICT, 2008): • **Zaballos, A. and Herranz, F. (2013)**
▪ **Awareness and Education** ▪ **Planning** ▪ **Notification** ▪ **Search &identification** ▪ **Dissemination and proof of evidence** ▪ **Hypothesis** ▪ **Examination** ▪ **Collection and storage** ▪ **External Entity of law, police and Global response**	• Cognizance of Cybercrime both by employees and the security teams • Planning involves both the internal and external entities • Awareness on cyber crime • Different security mechanisms in place • Defend their hypothesis using evidence collected • List of events clearly using the collected, documented information • scrutinized fully to get to all the tenacious details • This is information collected on cyber threat and should not be tampered • The existing environment in which cyber threat thrives in.	• Baker (2010) • Jacque, (2003) • Patel and Zaveri, 2010). • Reith, Carr and Gunsch - **Abstract model of computer forensic process** • Casey, E. (2000). • Longe O.B., Mbarika V.W., Jones .C. , Anadi .A., Wada (2010 (Real time model)
▪ **Governance** ▪ **People** ▪ **Training and Education** ▪ **Policies and processes** ▪ **Technology**	• legislation on Cybercrime • understanding of cyber by employee • Knowledge and skills on Cybercrime • Procedures and processes in place to combat cyber • Technical infrastructure in place to cyber	• United Nations report on Cybercrime 2013 • Baker (2010) • Jacque, (2003) • Patel and Zaveri, 2010)

From the input collected and as referenced on Table 3, below is the SMEs Conceptual model

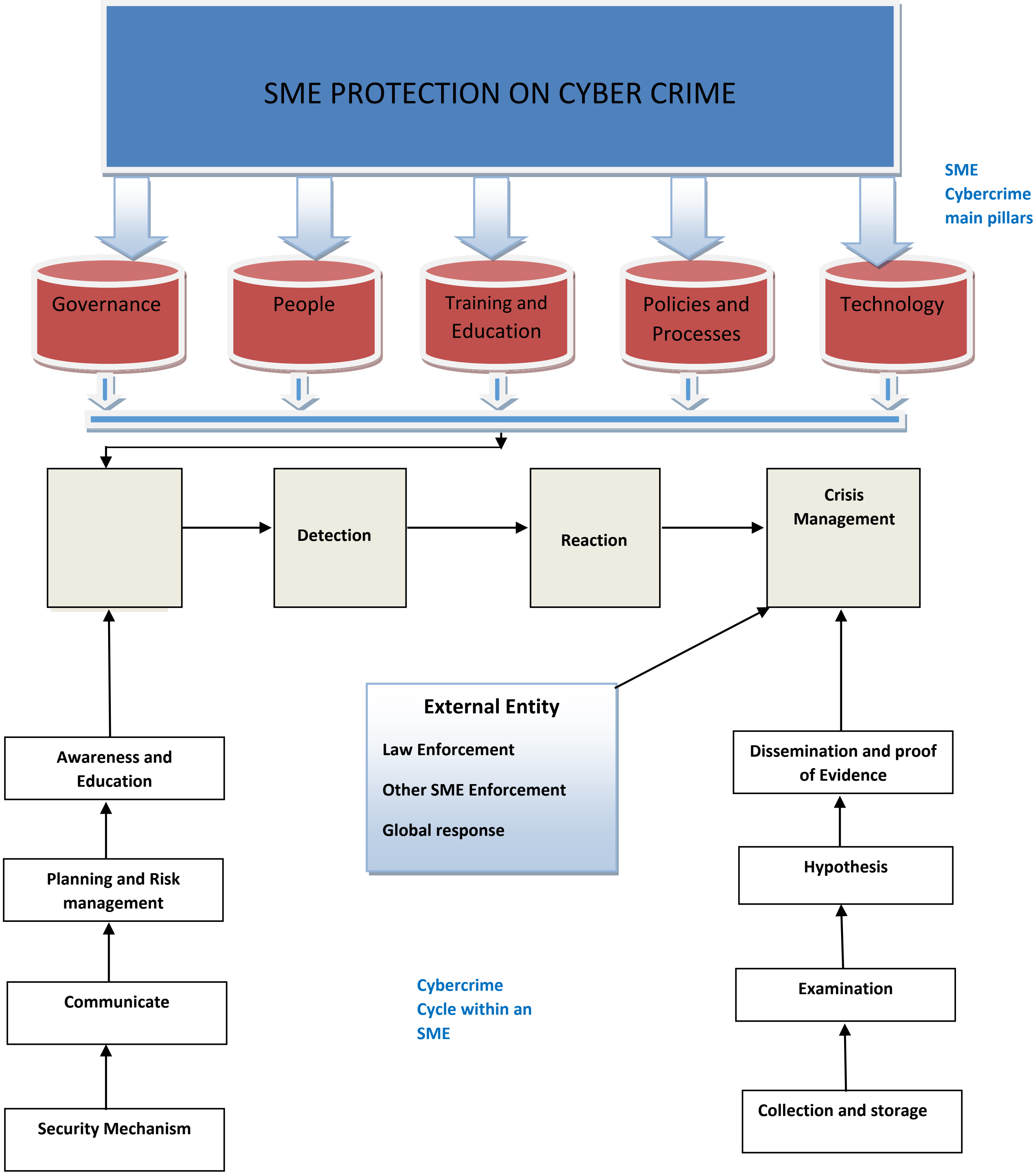


Figure7: Conceptual Model

2.9.6 Main Pillars for the Conceptual Model:

i. Governance

For governance, emphasis is put on the legislation on Cybercrime, law powers that will aim to investigate, prosecute Cybercrime offenses. In Kenya we currently have a Cybercrime and computer related crime bill Article 19 under the Kenyan law. The cyber bill is an initiative of the Office of the Director of Public Prosecution (ODPP). It seeks to equip law enforcement agencies with legal and forensic tools to tackle Cybercrime which has cost the country nearly 2 billion Ksh (23 million US dollars) in the year, June 2013. This is in accordance to the research conducted last year by (TESPOK) Telecommunication Service provider's association in Kenya. There has been a recommendation to improve this in accordance to the international standards especially in the area of protection of freedom of expression and privacy. Globally most countries have adapted the EU Convention on Cybercrime which is to act as the foundation point of reference from many countries when coming up with a Cybercrime bill.

According to Suter (2007) SMEs can minimize their manpower requirements by relying on a Nationally establish (CERT) Computer Emergency Response Teams to ensure that their security infrastructure is in check and that the ever growing threats on information systems is tackled.

International cooperation between parties is also a factor here as it helps to ensure that cyber criminals irrespective of the boundaries are profiled and are able to face the arm of the law in an event of a crime.

ii. Policies and Procedures

There is need for SMEs to ensure that they have put in place policies and procedures that will ensure that they have technical and social infrastructure in place to ensure that there is protection of their information systems and use. Most SMEs usually do not possess security and compliance policies (Kyobe, 2008), and a few engage in formal planning thus making most SMEs unable to handle security issues before hand.

We have different standards that have been put in place such as the ISO / IEC 27001 for small businesses which are at an affordable price and are customized to variant SMEs.

Rules and processes within the businesses should also put emphasis on the internal infrastructure and how communication should be done with the external entities.

iii. People, Training and Education

Baker, (2010) argues that the process of collection and analysis of Cybercrime data is often affected by a lack of understanding of what Cybercrime means or represents. Barker argues on how SMEs have become and continue to be the attacked by cyber criminals due to unawareness on the characteristics of Cybercrime in the event that there is an attack. Emphasis is put to have continuous training and education on Cybercrime and that employee should be on the lookout as they can be part of the attack from external entities.

iv. Technology

Conklin, (2008) looks at the technical infrastructure on businesses and how crucial this is in ensuring that cyber-attacks are curbed in variant ways. He reiterates the fact that emphasis should be done on the design of the security systems as these are profiled differently with unique applications and systems and that measures should be put in place especially for the SMEs when security infrastructure is being put in a piecemeal way.

Accepted standards should be used in SMEs security infrastructure and that there should be close liaison with the national (CERT) Computer Emergency Response Teams to ensure that security bridges are curbed before any imminent attack

The model is not complete unless the below activities are emphasized from the main pillars and put in place in the organization.

i. Prevention and Early warning

Computer attacks in SMEs manifolds itself in unique ways, but it is always prudent to have measures put in place as preventive and early warning both via policies and procedures within the business or via use of detective technological systems. This will go a long way reducing the number of information security breaches within the business. (UN-ESCAP, UNAPCICT, 2008):

Here the business has to identify the critical infrastructures within the business and ensure that their vulnerability to disruption is minimized and services are readily restored when disrupted. Prevention seeks to have activities in place that raise general preparedness of the business. This involves the dissemination of recommendations from other SMEs and businesses, and guidelines on best practices, timely and credible warning of specific threats, and the implementation of training and exercises.

Prevention of attacks gets its inputs from the main SME pillars but also it’s strengthened via continuous activities practiced by the SMEs.

a) Awareness and Continuous education

This is a major area of concern in this model as it focusses on cognizance of Cybercrime both by employees and the security teams. Most SMEs are attacked by Cybercrime repeatedly without any knowledge or allow or put themselves in situations that will allow an imminent attack. This model activity will focus on the continuous education on cyber activities to the target group and ensure that the security teams have put some security mechanisms that alerts them whenever of any cyber-attacks Baker (2010). The external or internal entities that assist the SMEs such as the auditing teams or the arm of the, need to be made aware when there is a problem or an attack on a particular business entity.

b) Planning and Risk management

Planning and Risk management involves both the internal and external entities. It goes straight way to ensure that the SME is able to secure the required infrastructure in place and that it has policies and procedures that caters for Cybercrime. It identifies the assets that are within the SMEs and ensures that it puts in place mechanisms to either prevent or mitigate cyber threat. External planning will focus on the legislature and regulations that are within the company’s boundary. This will extremely influence of the context on the Cybercrime in terms of monitoring and checking on evidence after it has occurred. (UN-ESCAP, UNAPCICT, 2008):

c) Communication / Notification

It is always prudent that the business is aware on the ongoing activities with regards to Cybercrime. This might be either with regards to an ongoing cyber theft or that employee to be on a watch out in case any suspicious activities reported. Suter (2007)

d) Security Mechanism

Search and identification step looks into the different security mechanisms in place; this might be in terms of firewalls, proxy servers in place to act as a security shield. It goes long way not only to search for details when there is an attack but also to ensure that the company is shielded from attacks such as denial of service through loop holes within the business. Suter (2007)

ii. Detection

This lays emphasis on the promotion of security and avoidance of vulnerable technologies. Here, new threats are to be discovered as an immediate concern and dealt with as quickly as possible. Zaballos, A. and Herranz, F. (2013).

In order for businesses to achieve deliverables from this pillar, there has to be internetwork of the SMEs and cyber security teams within governance that will identify the technical forms of attacks and cascade these to the rest of the teams to be on the lookout. SMEs can work together and have representatives who can investigate information on criminal organization as well as get support from government initiated bodies that are mandated to combat Cybercrime within the country. In addition, technical as well as non-technical information may need to be shared with international partners, since the threats to information security are not limited to geographic borders.

iii. Reaction

This focusses on the correction of the cause of disruption. SMEs should ensure that they have the incident response procedures as part of their company processes and policies. This should respond immediately to the attack as damage is usually dependent of how quick the attack is put on control. Zaballos, A. and Herranz, F. (2013).

Similar to the other pillars, reaction stage involves not only the technical measures but also focus will be on law enforcement as this will facilitate protection of others by increasing risk of capture in the event that the same attack was done in another SME. (UN-ESCAP, UNAPCICT, 2008).

iv. Crisis Management

Whenever a crime has been committed in an SME, the teams should always be closer to the decision making teams as this will be crucial. SMEs have to ensure they have in place crisis management plan and that this is rehearsed time to time so that everyone is familiar with their responsibilities, duties and roles in case of an attack.

Suter (2007) emphasizes the fact that Lessons learned should be exchanged with all critical players in order improve crisis planning and to streamline information-sharing in crisis situations. Companies and government sectors that were not affected by the attack can compare emergency plans and take steps to avoid mistakes.

This stage is not complete until evidence is collected in the event of the crime. This is why the SMEs will have to have a further understanding on the below action steps,

i. Collection and Storage

This is information collected on cyber threat. This might be from external entities or within when audit is done in an event to ensure that structures are in place to combat with Cybercrime and in an event of any attack, information can be collected for the same. Good Storage provides a hive that one is able to refer to material that is not interfered or tampered with the confidentiality, integrity or authenticity of the collected information. Reith, Carr et al (2002).

ii. Examination

In examination different techniques and tools are put in place to ensure that the information collected or evidence is scrutinized fully to get to all the tenacious details that might either act as evidence on a cyber-attack or might be a loop hole that might make the business vulnerable to cyber-attacks. Reith, Carr et al (2002).

iii. Hypothesis

The teams are able to collect evidence or information of value that they are able to act upon to prevent any attacks on their security infrastructure. Basing on the kind of information that they have collected, the teams can come up with a hypothesis on the list of events clearly using the collected, documented information that the teams have. This can either be done by the external entities e.g. Police if there is a crime that is being investigated or internally by auditors in an event of ensuring that everything is working in accordance to the stipulated rules and guidelines. Reith, Carr et al (2002).

iv. Dissemination / Proof of Evidence

In cases where an act of crime has occurred, one is required to defend their hypothesis using evidence collected. This acts as their proof of evidence and one is able to backtrack on the previous steps to ensure that they are able to back up their hypothesis. The information retrieved has to be disseminated to the correct target group, within or without the organization for action. This is to ensure that if there are any loopholes they are dealt with or in cases where evidence has been collected action is taken against the masterminds in courts. Reith, Carr et al (2002).

2.9.7 Model Evaluation

This model has been validated by presenting it to the experience personnel within SMEs that deal with security infrastructure or internet attacks both internal and external experts within the SMEs. Here, the model was presented and depending on the environment that the business is working under will be able to have variant perspective in focus or different views of the subject matter. Various variables were put into consideration and whether it would make sense especially within the target group which is SMEs.

Questions arising from the model and discussion around it will was done via questionnaires; interviews thus this enabled full advantage of the team in charge.

Since the questionnaires to the target group focused on the variables in question, some activities were conducted on the same such as Cronbach alpha and use of coefficients to establish the relationship between variables.

CHAPTER THREE

3.0 METHODOLOGY

3.1 Introduction

In this chapter, we've looked at the tools and methods that were used in the research. Research design, defined as a "blueprint" was used in this study as a framework from which the research methodology was drifted from. It brought together claims that are being made about what constitutes knowledge, a strategy of inquiry and specific methods. Usually three approaches can be used to enable one carry out their research and these are qualitative, quantitative or mixed methods (Cresswell 2003). Kothari (2004) defines it as the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure.

In this particular study, we've employed both qualitative and quantitative research methodologies that has seen us get a total of 93 valid questionnaires out of the 106 issued out in the study. One of the objectives of this study was to understand the measures put in place for cyber-attacks for SMEs with an online presence and the strength and weaknesses of these initiatives and come up with a framework that has been applicable for the SMEs.

Seeking to unravel the employee opinion and understand the current activities in the small businesses was made possible using qualitative methodologies. Quantitative method has ensured that the research retrieves statistics from the selected SMEs and tangibility of information collected. (Ritchie and Liz Spencer, 2002).

3.2 Target Population and Scope

A population refers to the sum of individuals or events from which a sample is drawn. (Mugenda and Mugenda, 2003). In this study, target population was SMEs that have an online presence in Nairobi, this is as a result that more than 50% of SMEs in the country are in Nairobi County and those with different branches have their headquarters in the city. (GoK 2007).

The target findings focused on employees, procedure, processes existing and how best a Cybercrime model can strengthen the existing measures to curb Cyber-attacks.

3.3 Sampling technique and Sample size

Simple random sampling and applied stratified technique was used in this study.
Both Mugenda and Mugenda, (2003) and Kothari (2004) suggest statistical formula for arriving on a sample size.

i. Margin of Error (Confidence Interval); this is the percentage of error to allow in the sample. In this study we shall use 8% margin of error
ii. The confidence interval determines how much higher or lower than the population mean you are willing to let your sample mean fall.
iii. Confidence Level; was the degree of confidence for the actual mean. The most common confidence intervals are 90% confident, 95% confident and 99% confident.

    This formed part of the constant value in the equation for the sample size

    (Z as a constant value)

    - 90% – Z Score = 1.645
    - 95% – Z Score = 1.96
    - 99% – Z Score = 2.576
iv. Standard of Deviation was the expected variance in the responses when conducting the research. In this study we used standard deviation of .5

Necessary Sample Size = (Z-score) ^{2} * StdDev*(1-StdDev) / (margin of error)^2

$((1.645)^2 \text{ x } .5(.5)) / (.08)^2$

105.7

Thus sample size for this study focused on 105.7 participants.

3.4 Research Instruments

The researcher used questionnaire to collect primary data from respondents. Closed ended questions were applied to collect quantitative data. The questionnaires were distributed to the respondents manually and collected after. Interviews sessions were applied especially for the managerial level team that is responsible for decision-making with regards to technology in the businesses.

During the interview sessions, the researcher allowed the respondents to say what they feel to maximize their self-disclosure, only injecting when the respondents are unclear or repetitive. The researcher also endeavored to be adaptive and flexible in technique. (Robins, 1997).We had a total of 93 valid questionnaires used, out of the 106 issued out in the study. Participant observation was also used to collect any day-to-day recovery activities undertaken. Secondary data came in handy especially in cases where one is needed to gain further understanding on the kind of business the SME deals with and how best the conceptual model will suit their current needs on Cybercrime.

3.5 Data Presentation and Analysis

The data collected using questionnaires was classified and coded numerically in order for the data to be manipulated and analyzed. Descriptive statistics was used to analyze the data. This type of scale is used to measure values, opinions and attitudes with regards to the technology, and measures put in place to curb Cybercrime. (Saunders, et al 2001).The method uses numbers and descriptions to rank or rate. The ratings of this methods range from strongly agree to strongly disagree. Data was analyzed according to the questions and was weighed as follows; strongly agree, agree, neutral, disagree and strongly disagree. Concerning the in-depth interviews, the researcher used Miles and Huberman approach that has the following traits; data reduction, data display and conclusion drawing and verification.

3.6 Ethical Considerations

The research upheld all ethical issues expected in the design, conduct, analysis and dissemination in the entire study. Participants were informed of the purpose of the study seek their consent prior to their participation. Accurate standards were adhered to in the collection, analysis and interpretation of the study findings. Ethics pertaining to the academic writing and publishing has been enforced.

3.7 Validity and Reliability

Validity is establishing whether the instrument content is measuring what it is supposed to measure (Mugenda, 1999) Reliability is the extent to which operations of the study will yield consistent results or data after repeated trials. For this study, we conducted a parallel test reliability of the instruments to the targeted SMEs with similar characteristics to the target group. This assisted us greatly in instrument enhancement, thus reliability.

CHAPTER FOUR

4.0 FINDINGS ANALYSIS AND INTERPRETATION

4.1 Introduction

The purpose of the data analysis and interpretation phase is to transform the data collected into credible evidence about the development of the intervention and its performance. (ICAP 2015)

Data collected in this study was gathered through questionnaire and interviews. The questionnaire and the questions asked in the interviews were designed in line with the objectives of the study. In this chapter, both qualitative and quantitative data was applied to enhance quality of data obtained, Likert type questions were also included whereby respondents indicated the extent to which the variables were practiced or challenges encountered.

This stage focusses on collecting data to test reliability and validity of the conceptual model. The research findings and interpretation from data collected from the findings are represented in parametric statistical methods that will involve cross tabulation, reliability and validity analysis and correlation matrices.

4.2 Data processing and Analysis

Data processing will involve the editing, coding and classification and tabulation of the collected data. It is the manipulation of items of data to get meaningful information (Carl, 1996).

Data analysis makes use of specialized and highly accurate algorithms and statistical calculations that are less often observed in the typical general business environment. McCleland, et al (1989).

Data processing uses numerical representation and items of data are stored as integers, whereas for data analysis details here are stored as floating point's representations.

It uses data analysis packages like SPSS or SAS, or their free counterparts such as DAP, PSPP are often used (Carl, 1996).

One is able to get patterns or relationships from computation of the collected coded data. In this survey we had a total of 106 participants to the questionnaires issued. We eliminated wrongly filled, some were incomplete and left us with 93 valid questionnaires.

4.3 Coding Responses

In this study, data was analyzed using SPSS where the closed ended questions were assigned numbers and for the open ended, themes were identified as through the collected questionnaire feedback and from these themes we were able to come up with the coded patterns this is as defined in section 4.6 KMO and Bartlett's Test.

4.3 Description of Reliability and Validity testing

4.3.1 Reliability

Cozby, P.C. (2001) states that, reliability is the degree to which an assessment tool produces stable and consistent results.

We have different types of reliability such as Test-retest reliability is a measure of reliability obtained by administering the same test twice over a period of time to a group of individuals.

Parallel forms reliability is a measure of reliability obtained by administering different versions of an assessment tool (both versions must contain items that probe the same construct, skill, knowledge base, etc.) to the same group of individuals. The scores from the two versions can then be correlated in order to evaluate the consistency of results across alternate versions. Phelan (2005)

In this study, due to time construct, parallel forms of reliability were highly used as one could easily probe the same question in a different way and to determine whether similar answers are obtainable.

4.3.2Validity

For a test to be reliable, it also needs to be valid. Validity refers to how well a test measures what it is purported to measure. Phelan (2005). In this study, we have different forms of validation.

Face Validity ascertains that the measure appears to be assessing the intended construct under study. The stakeholders can easily assess face validity although not scientific, it’s an essential component.

Construct Validity is used to ensure that the measure is actually measure what it is intended to measure (i.e. the construct), and not any other variables. (Wren, 2005)

Sampling Validity (similar to content validity) ensures that the measure covers the broad range of areas within the concept under study. Not everything can be covered, so items need to be sampled from all of the domains. In this study, the items that form basis of discussion will careful be selected even as we approach the technical experts in the world of technology. (Wren, 2005)

Data collected from the field involved small and medium businesses dealing with website designers, domain name resellers, information services professional, software resellers, web advertisement companies, premium rate services companies, application developers, electronic shopping websites, social online sellers, resume-cover letters writers, electronic marketers and consulting firms.

4.4 Reliability Analysis of collected data

The sample SPSS test output shows that our tool is reliable because the cronbach alpha of 0.761 is greater than the recommended 0.7 variance. This shows as per Table4 that we can actually use the instrument to proceed in our studies

Reliability Statistics

Cronbach's Alpha	N of Items
.761	14

Table 4: Reliability statistics for the collected data in the study Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Experience in handling cybercrime	32.54	23.295	.426	.741
Computer reference points	32.78	22.453	.652	.718
Triggers for computer upgrades and updates	32.78	22.453	.652	.718
What security check is assessed	32.94	25.844	.329	.752
Computer as a daily function	30.58	26.137	.483	.749
Number of computers in use	32.14	22.448	.549	.727
Responsible teams handling security	32.26	24.107	.248	.766
Resources allocated to cybercrime	32.05	26.008	.188	.763
Virus attacks	33.47	27.774	.000	.765
Fraud attacks	32.17	24.405	.278	.759
Internet as a daily routine	30.58	26.137	.483	.749
Other attacks	31.14	22.143	.336	.763
Any changes done after attack	30.57	25.791	.425	.748
Number of Employees	32.14	22.448	.549	.727

Descriptive Statistics

For descriptive statistics we were also able to ascertain that the questionnaire used was reliable due to the fact that values retrieved for Correlation matrix between significantly two variables indicated a strong linear relationship of values 0.446 as depicted in table 5; the more knowledgeable one is in handling Cybercrimes, the better his reference points in tackling Cybercrime.

Table 5: Descriptive statistics for reliability

	Mean	Std. Deviation	N
Experience in handling cybercrime	1.94	.895	93
Computer reference points	1.69	.766	93

Correlations

		Experience in handling cybercrime	Computer reference points
Experience in handling cybercrime	Pearson Correlation	1	.446**
	Sig. (2-tailed)		.000
	N	93	93
Computer reference points	Pearson Correlation	.446**	1
	Sig. (2-tailed)	.000	
	N	93	93

**. Correlation is significant at the 0.01 level (2-tailed).

4.5 Validity analysis of Collected Data

To ascertain the convergent and discriminant validity of the test instrument, factor analysis was done. This is the statistical measure to analyze the interrelationship among large number of variables and explain underlying dimensions. In factor analysis, if these items load together, it represents similar areas of concern. Factor analysis for each questionnaire generated using principal component extraction and Promax rotation. Type of rotation to use depends your perception with regards to the data whether the variables in place are correlated to each other or not. Promax, will include un-correlation data as per Table

Table 6: Statistical measure to analyze relationship among large number of variables

Correlation Matrix

		Number of Employees	Computer as a daily function	Triggers for computer upgrades and updates	Experience in handling cybercrime	Resources allocated to cybercrime	Basic firewall and encryption
Correlation	Number of Employees	1.000	.411	.367	.333	.200	.146
	Computer as a daily function	.411	1.000	.268	.209	.164	.206
	Triggers for computer upgrades and updates	.367	.268	1.000	.446	.024	-.034
	Experience in handling cybercrime	.333	.209	.446	1.000	.045	.129
	Resources allocated to cybercrime	.200	.164	.024	.045	1.000	.019
	Basic firewall and encryption	.146	.206	-.034	.129	.019	1.000
Sig. (1-tailed)	Number of Employees		.000	.000	.001	.027	.081
	Computer as a daily function	.000		.005	.022	.058	.024
	Triggers for computer upgrades and updates	.000	.005		.000	.409	.375
	Experience in handling cybercrime	.001	.022	.000		.335	.109
	Resources allocated to cybercrime	.027	.058	.409	.335		.429
	Basic firewall and encryption	.081	.024	.375	.109	.429	

a. Determinant = .473

We had some items with a fair high correlation such as triggers for computer upgrades and experience in handling Cybercrime. In statistics, if you get a correlation matrix of an item by the other as 1 it means that the items are representative of a similar scenario and that one variable should be removed.

In our findings, we established correlation of the items using the determinant, (It has to be greater than .00001, shown in table 7) the determinant here was .473.

Table 7:KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.664
Bartlett's Test of Sphericity	Approx. Chi-Square	66.772
	df	15
	Sig.	.000

Statistical significance of collected data via KMO

For KMO we got a value of .664 , any value above .5 and greater the better, For statistical significance we've got it covered in the analysis as we have a value of .000 value less than .001

Table 8:Total Variance Explained, Extraction method

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	2.111	35.182	35.182	2.111	35.182	35.182	1.969
2	1.099	18.313	53.495	1.099	18.313	53.495	1.537
3	.998	16.638	70.133				
4	.739	12.325	82.457				
5	.554	9.233	91.691				
6	.499	8.309	100.000				

Extraction Method: Principal Component Analysis.

a) When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

To ascertain the convergent and discriminant validity of the test instrument, factor analysis was done. There are two components that were extracted based on the Eigen value of greater than 1. The two components explain the total value of variance which is 53% as per table 8.

The below table 9 and 10 shows the variables and which component they fall in, either one or two.

Table 9: Component Matrixa

	Component	
	1	2
Number of Employees	.764	.091
Computer as a daily function	.669	.308
Triggers for computer upgrades and updates	.682	-.511
Experience in handling cybercrime	.673	-.357
Resources allocated to cybercrime	.283	.518
Basic firewall and encryption	.287	.582

Extraction Method: Principal Component Analysis

a. 2 components extracted.

Table 10: Pattern Matrix[a]

	Component	
	1	2
Number of Employees	.545	.392
Computer as a daily function	.319	.567
Triggers for computer upgrages and updates	.900	-.232
Experience in handling cybercrime	.785	-.084
Resources allocated to cybercrime	-.135	.620
Basic firewall and encryption	-.176	.685

Extraction Method: Principal Component Analysis.

Rotation Method: Promax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

The pattern matrix these values for the component load together fairly tightly/seem to represent same value, hence the value pattern seems to show two distinct patterns.

4.6 Variable Analysis

To make data more representative we grouped it according to areas that represent governance, people, technology, policies and procedures and training and education.

4.7.1 Computer reference points

In the collected findings in table 11, we were able to confirm that most of the SMEs are able to initiate upgrades or updates due to information they get from friends, other businesses or the internet. This represents about 50% of the total sample population.

Table 11: Triggers for computer upgrades and updates * Computer reference points Cross tabulation

Count

		Computer reference points			
		Internet and friends	Internet and professional expert	Internet, friends and computer magazines	Total
Triggers for computer upgrades and updates	Internet and friends	46	0	0	46
	Internet and professional expert	0	30	0	30
	Internet, friends and computer magazines	0	0	17	17
Total		46	30	17	93

Bar chart representation for computer reference point:

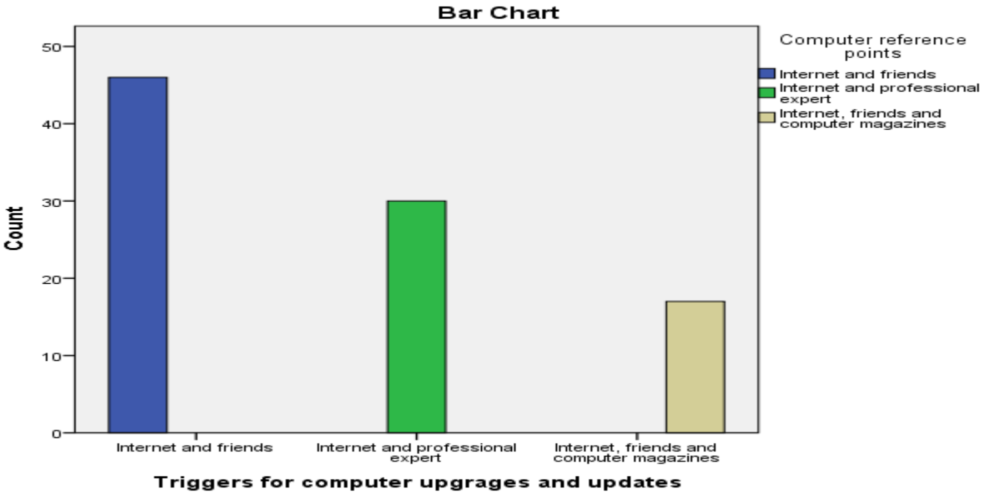


Figure 8: Triggers for computer upgrades and updates

4.7.2 Basic firewall and encryption

One of the activities that are being done to curb Cybercrime is having a basic firewall in place and applying encryption mechanisms. We released that 35% of the target group as shown in Table 12, would desire to enforce some security mechanisms but unable due to limited resources.

Table 12: Triggers for computer upgrades and updates * Basic firewall and encryption Cross tabulation

Count

		Basic firewall and encryption			
		Resource limit but desirable	Enforced	Enforced with close monitoring	Total
Triggers for computer upgrades and updates	Internet and friends	16	16	14	46
	Internet and professional expert	9	6	15	30
	Internet, friends and computer magazines	8	5	4	17
Total		33	27	33	93

4.7.3 Password protected PC and antivirus protection

93% of the target group enforces password and antivirus protection. The below table 13,depicts the different triggers.

Table 13: Triggers for computer upgrades and updates * Password protected PC and Antivirus Cross tabulation

Count

		Password protected PC and Antivirus			Total
		Resource limit but desirable	Enforced	Enforced and close monitoring	
Triggers for computer upgrades and updates	Internet and friends	0	42	4	46
	Internet and professional expert	2	28	0	30
	Internet, friends and computer magazines	0	17	0	17
Total		2	87	4	93

4.7.4 Responsible teams in handling security

In the findings, we had over 33% of SMEs having team leads as experts and responsible for handling computer security issues in the business. Table 14 indicates the triggers for computer upgrades or security updates and the teams responsible for handling it.

Table 14: Triggers for computer upgrades and updates * Responsible teams handling security Cross tabulation

Count

		Responsible teams handling security				
		Team business lead	IT Expert	Outside IT Expert	Everyone’s responsibility	Total
Triggers for computer upgrades and updates	Internet and friends	25	4	8	9	46
	Internet and professional expert	2	19	8	1	30
	Internet, friends and computer magazines	4	0	11	2	17
Total		31	23	27	12	93

Bar graph presentation

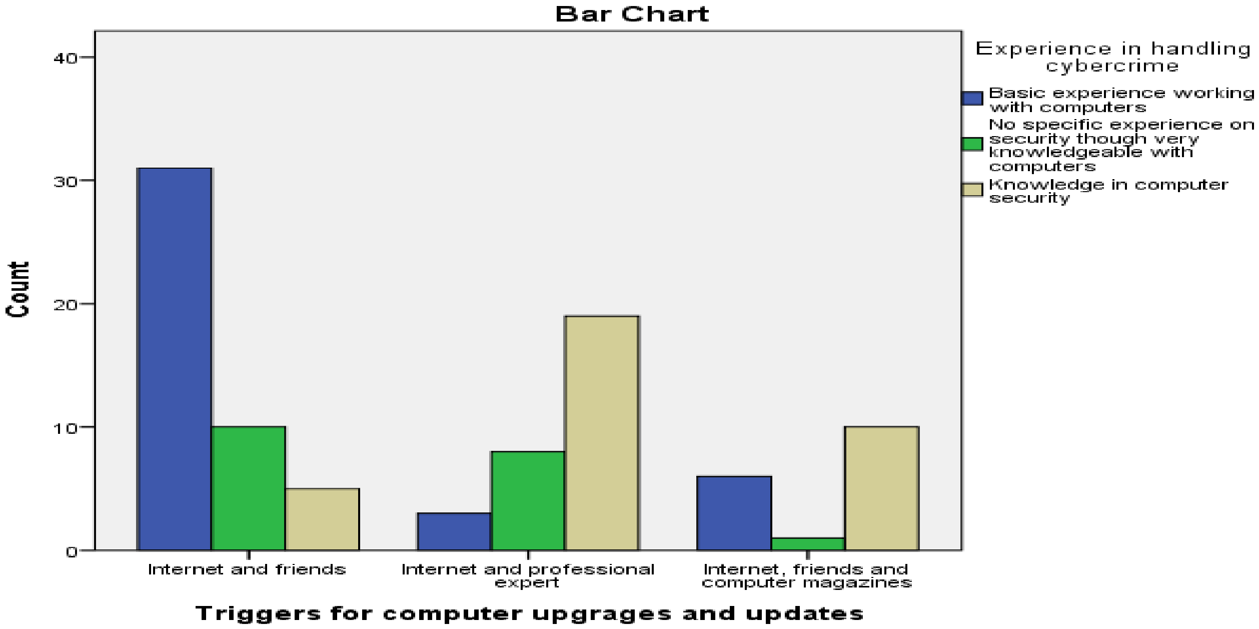


Figure 9: Triggers for computer upgrades and updates

4.7.5 Experience

Most of the SMEs established and running businesses on the internet got experience by working with computers and are not professional. This according to Barker (2010) might cause them lack understanding what Cybercrime is and how to mitigate, prevent themselves from attacks.

Table 15: Triggers for computer upgrades and updates * Experience in handling cybercrime Cross tabulation

Count

		Experience in handling cybercrime			
		Basic experience working with computers	No specific experience on security though very knowledgeable with computers	Knowledge in computer security	Total
Triggers for computer upgrades and updates	Internet and friends	31	10	5	46
	Internet and professional expert	3	8	19	30
	Internet, friends and computer magazines	6	1	10	17
Total		40	19	34	93

4.7.6 Government in Cybercrime

According to Suter (2007) SMEs can minimize their manpower requirements by relying on a Nationally establish (CERT) Computer Emergency Response Teams to ensure that their security infrastructure is in check and that the ever growing threats on information systems is tackled. From data that there is a significant gap in what the government is doing and no impact on manpower is being felt by the SMEs.

We see over 83% of feedback from table 16 and figure 10 that the SMEs disagree in government efforts towards Cybercrime.

Table 16: Triggers for computer upgrades and updates * Government assistance in Cybercrime Cross tabulation

Count

		Government assistance in Cybercrime		Total
		disagree	agree	
Triggers for computer upgrades and updates	Internet and friends	36	10	46
	Internet and professional expert	25	5	30
	Internet, friends and computer magazines	17	0	17
Total		78	15	93

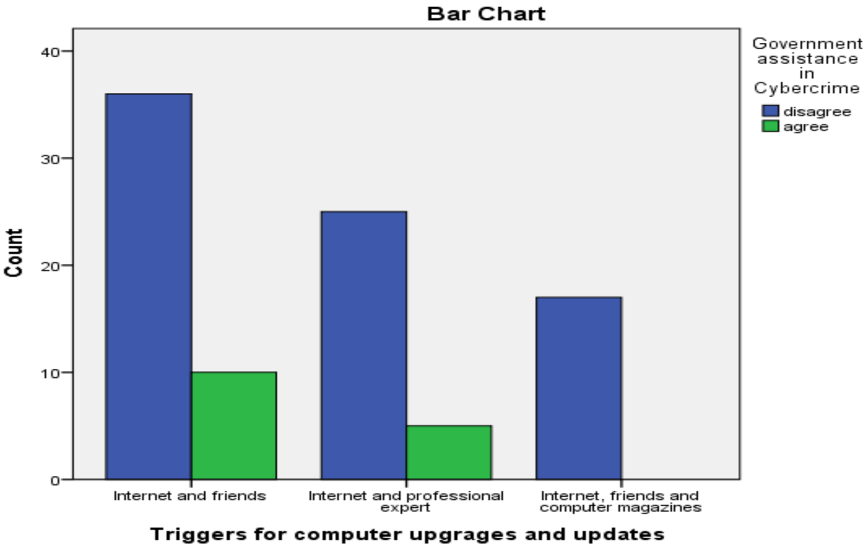


Figure 10, Government assistance in cybercrime,

4.7 Security Check Schedules

4.8.1 Computer level of access

In this finding it was noted as shown in table 17, that the educational level for SMEs on Cybercrime is wanting and that it is evident that the target group requires training on the same. Out of a total of 93 SMEs that were targeted, 68% of these are okay to have same level computer systems access in their businesses.

Table 17:Security check schedules * Is it okay to have same level of computer access Cross tabulation

Count

		Is it okay to have same level of computer access				Total
		strongly disagree	disagree	agree	strongly agree	
Security check schedules	when there has been an attack	0	4	19	2	25
	12 months or when there has been an attack	3	6	14	0	23
	6 months or when there is an attack	0	3	13	1	17
	Occasional or when there is an attack	0	8	18	2	28
Total		3	21	64	5	93

4.8.2 Security checks in the SME

Most checks for baseline controls done when there has been an attack. SMEs should have a more frequent check on systems to mitigate and avoid imminent security attacks. See below table 18,

Table 18:Security check schedules * What security check is assessed Cross tabulation

Count

		What security check is assessed		Total
		Baseline controls	System specific and baseline controls	
Security check schedules	when there has been an attack	16	9	25
	12 months or when there has been an attack	7	16	23
	6 months or when there is an attack	6	11	17
	Occasional or when there is an attack	14	14	28
Total		43	50	93

4.8.3 Virus Attacks

All SMEs reported to have been attacked by viruses in one way or the other. Table 19 depicts the security check schedules and the number of virus attacks.

Table 19:Security check schedules * Virus attacks Cross tabulation

Count

		Virus attacks	Total
		frequent	
Security check schedules	when there has been an attack	25	25
	12 months or when there has been an attack	23	23
	6 months or when there is an attack	17	17
	Occasional or when there is an attack	28	28
Total		93	93

4.8.4 Hacking Attacks

Hacking also proved to be frequent, some of the SMEs confirming that there are instances where they are not sure whether they've been hacked or not. Table 20 shows the security check schedules and the hacking frequency.

Table 20: Security check schedules * Hacking attacks Cross tabulation

Count

		Hacking attacks			Total
		Frequent	Occasional	Not sure	
Security check schedules	when there has been an attack	21	0	4	25
	12 months or when there has been an attack	19	1	3	23
	6 months or when there is an attack	15	0	2	17
	Occasional or when there is an attack	13	3	12	28
Total		68	4	21	93

4.8.5 Fraud Attacks

In the findings under fraud, 61% of the SMEs were not sure whether at some point they have been victims of this kind of attack, but they've heard, their customers complaining of being compromised on the online system. Security check schedules shown in the below table 21.

Table 21: Security check schedules * Fraud attacks Cross tabulation

Count

		Fraud attacks			Total
		Frequent	Occasional	Not sure	
Security check schedules	when there has been an attack	6	1	18	25
	12 months or when there has been an attack	9	2	12	23
	6 months or when there is an attack	3	1	13	17
	Occasional or when there is an attack	11	3	14	28
Total		29	7	57	93

4.8.6 Encryption

The below table 22 indicates the security check schedules and the frequency experienced in the cyber-crime encryption attacks.

Table 22: Security check schedules * Encryption attacks Cross tabulation

Count

		Encryption attacks			Total
		Frequent	Occasional	Not sure	
Security check schedules	when there has been an attack	5	3	17	25
	12 months or when there has been an attack	7	6	10	23
	6 months or when there is an attack	6	3	8	17
	Occasional or when there is an attack	4	2	22	28
Total		22	14	57	93

4.8.7 Other Attacks

Table 23: Security check schedules * Other attacks Cross tabulation indicating DOS, mail spam, hacking and computer worms.

Count

		Other attacks					
		Denial of service	Mail spam	Hacking	Worms	none	Total
Security check schedules	when there has been an attack	1	1	11	4	8	25
	12 months or when there has been an attack	2	1	7	10	3	23
	6 months or when there is an attack	3	1	4	6	3	17
	occasional or when there is an attack	8	0	11	4	5	28
Total		14	3	33	24	19	93

4.8.8 System security changes done after attack

In all these kinds of attack, only 5% in the selected sample target, demonstrated change that occurred after they had a cyber-attack. 95% have done little or no change from the previous cyber-attack.

Table 24: Security check schedules * Any changes done after attack Cross tabulation

Count

		Any changes done after attack				
		Every day antivirus updates	Yes became more aware of incoming email	Frequent antivirus updates	No much change	Total
Security check schedules	when there has been an attack	1	1	2	21	25
	12 months or when there has been an attack	0	0	0	23	23
	6 months or when there is an attack	0	0	2	15	17
	occasional or when there is an attack	0	0	0	28	28
Total		1	1	4	87	93

4.8 Cybercrime Model for SMEs

The level of cyber-attacks on organizations has increased tremendously in recent years. When such attacks occur, organizations need to assess the damage and loss from this crime. While large organizations have the mechanisms to determine such losses, SMEs lack such capability and often ignore the need to implement effective information security measures (Kyobe, 2008;) The government can strongly support the SMEs especially with use of the CERT systems in place, depending on the SMEs nature they can get advice and support in an event of a cyber-attack.

From the findings, most SMEs do not comply with the existing Information security management standards such as the ISO 27001.The standards have provision to assist the businesses have a robust information security framework to guard against Cybercrime attacks. SMEs can always engage with the national bodies in place and establish the right ISO processes and procedures targeted for SMEs that they can adapt in their businesses. We have different standards that have been put in place such as the ISO / IEC 27001 for small businesses which are at an affordable price and are customized to variant SMEs.

Most SMEs fall victims of Cybercrime attack due to their business model Clarke (1997). We find that due to their nature, SMEs usually minimize their Information technology costs to a point that they outsource their technology services, they are heavy on Cloud services and sometimes some employees' BYOD (bring their own devices), with such model in place there is a need to ensure that they have the right security infrastructure in place such as the baseline controls depending on their business models types.

Their low cutting budget causes them to be victims of software piracy and trade and logo attacks as they might not be able to sniff out illegal use of their trademarks in the internet as corporates. SMEs have to ensure that they get the right software for their businesses this will minimize their vulnerability and at the same time avoiding software piracy a menace to the society.

Risk management is also key and the goal is to identify, measure, control and minimize losses associated with uncertain events (Patel and Zaveri, 2010). Most SMEs do not conduct risk management process in their companies, hence there is no assessment done that can help them identify their weak point and mitigate against this, hence an action point and one of the processes that should be enforced by all SMEs.

According to Suter (2007) SMEs can minimize their manpower requirements by relying on a Nationally establish (CERT) Computer Emergency Response Teams to ensure that their security infrastructure is in check and that the ever growing threats on information systems is tackled.
Emphasis should be done on the design of the security systems as these are profiled differently with unique applications and systems and this should be keenly addressed especially when SMEs put their security infrastructure in a piecemeal way.

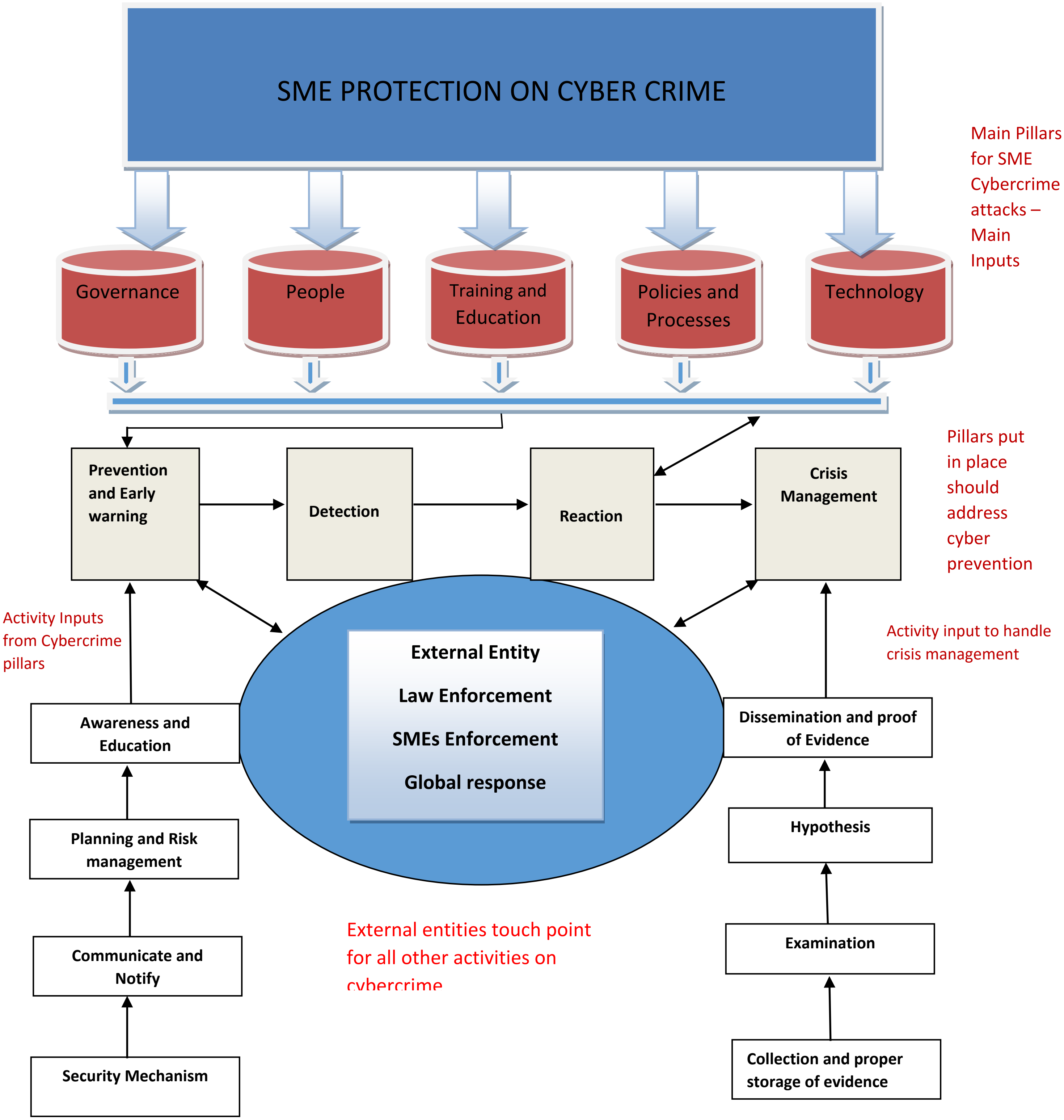
The final model realized is unique to SMEs as its focusing on the weakened areas in an SME setting that is highly likely to make them targets of Cybercrime as compared to the large organizations.

Emphasis is put on training and education as most SMEs lack the qualified personnel as technology experts in their security system infrastructure hence the need to understand the basic baseline controls needed in their businesses to counter Cybercrime attacks.

4.9.1 Cybercrime Model as compared to conceptual model

From the data collected and analyzed, it is clear that SMEs need to adapt to a model that will enable them be proactive enough to prevent cyber-attacks and in the even that this was to happen, to detect as quickly and ensure that it restores back the services to normal.
The SMEs cybercrime model as shown in figure 11 below, is emphasizing the fact that for us to make it more effective, we need to work closely with the government entity, with other SMEs within the same region within or without and the fact that global response and warning is also crucial in our fight against cybercrime.
This has been emphasized on the model by having a close liaison of the external entity in relation to of all other internal activities, such as prevention, detection or reaction of cyber-crime.

Cyber Crime Model for SME



Main Pillars for SME Cybercrime attacks – Main Inputs

Pillars put in place should address cyber prevention

Activity Inputs from Cybercrime pillars

Activity input to handle crisis management

External entities touch point for all other activities on cybercrime

Figure 11: Cybercrime Model for SME

CHAPTER FIVE

5.0 Conclusion and Recommendation

Over the years, most businesses react to cyber security threats which should not be the case. E-Businesses have waited for crimes to occur and tackling with a perception of a non-reoccurrence. We need a more proactive approach with dealing with Cybercrime insisting on more formal preventive measure than reactive. This can be accomplished majorly via awareness, information sharing for various segments of SMEs and ensuring that exists preventive frameworks with an acceptable security levels for different e-businesses

The main objectives of this research was to establish the seriousnes of SME Cybercrime, measures put in place for cyberattacks, and to come up with a model for SMEs. From the data collected it was established that we have seveal upcoming SMEs E-businesses with low security for internet access. Over 80% of businesses have not secured their elecronic webpages to counter Cybercrime attacks such as phishing under their web accounts. Over 90% of SMEs e-businesses have encountered cyber attacks in one way or the other but have not taken any measures after the attack to ensure that similar attacks in future do not reoccure. More than 50% of SMEs lack knowledge and training on cyber crime and how best they can deal with issues arising from it. Some measures have been put forth such as baseline security controls eg. Antivirus which do not comprehensively deal to the ful the menance. Risk analysis is key to ensure that the main focus assests of the business is well taken care of as it might not be possible to cater for all assets order of priority can be put for the most crucial areas of immeninent attacks.

It is impractical to identify all threats that could occur, but its possible to come up with a set of base controls that detect major cyber security threats, minimize their occurances and effects.

Government can play a major role in supporting SMEs especially those specializing on e-commerce. They can organize for major training and support for different SMEs representative, this can be done in a way that the same is relayed or cascaded to other teams/groups of SMEs. The CERT teams can come in handy, and ensure that it communicates or shares cyber threat information to SMEs this will enable them be on the look out and put the right mechanims to stop any forms of attacks. Since cost is an issue for SMEs, this will enable them reduce their costs for manpower in their work streams and at the same time rely heavily on law enforcement whenever such acts are committed.

Article 19 of the laws of Kenya talk about computer crimes and laws governing this. It has been criticised that it lacks freedom of expression, Kenyan government should be able to adopt to the European convention on cyber crime and ensure that it works with government across as cyber crime is a borderless crime and countries should work together in the fight against crimes committed in this nature.

Attitude of SMEs management towards cyber crime is key, all the above can be put in place but if the management attitude is negative, there will be less or no effort put towards Cybercrime threats. We need to have continous workshops that talk about Cybercrime and how best this can be improved from the existing practises wherer cyber crime is not taken seriously.

5.1 Further Research

This research has focused on all types of SMEs who conduct their business online. There is need to do further research on SMEs dealing with one line of business and to investigate further on the attacks and how best this can be managed.

More investigation is needed to understand the impact of some activities on SMEs eg. Government related or Risk management related and how best this can ensure that we mitigate SMEs attacks.

REFERENCES

Adarsh Kansal , Ankit Sikka, Ankit Gupta 2014 volum 3Dronacharya college of engineering, Greater Noida (U.P), INDIA Mahamaya Technical University

Baker, W.H. (2010). Thoughts on Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Mapping and Measuring Cybercrime

Beckett, H., (2003). ComputerWeekly.com, *SME nation: an IT strategy for the future*,

Brenner, S. (2007), "Law in an Era of Smart Technology", Oxford: Oxford University Press.

Carl, F (1996). *Data Processing and Information Technology (10th ed.)*. Thomson. p. 2.

Casey, E. (2000). Digital Evidence and Computer Crime. San Diego: Academic Press.

Chawki, M. (2009). Nigeria Tackles Advance Free Fraud. Journal of Information Law & Technology (2009) No. 1. Retrieved January 12, 2010 from http://go.warwick.ac.uk/jilt/2009_1/chawki

Chaffey, D. (2009). E-business and E-commerce Management: Strategy, Implementation and Practice (4th Edition). England: Pearson Education Limited.

Charmayne, C., (2001) Computer Crime, Vulnerabilities of Information Systems, and Managing Risks of Technology Vulnerabilities, Pearson, USA.

Clarke, R. V. and M. Felson (Eds.) (1993). Routine Activity and Rational Choice. Advances in Criminological Theory, Vol 5. New Brunswick, NJ: Transaction Books.

Ciardhuáin, S. (2004) An extended model for Cybercrime investigations; International Journal of digital Evidence Summer 2004, Volume 3, Issue 1.

Conklin, W. A., and Dietrich, G. (2008, January 7). Systems Theory Model for Information Security. Proceedings of the 41st Hawaii International Conference on System Sciences - 2008, (pp. 1-9). Big Island, Hawaii.

Colin Phelan and Julie Wren, Graduate Assistants, UNI Office of Academic Assessment (2005-06).

Cozby, P.C. (2001). Measurement Concepts. Methods in Behavioral Research (7th ed.).

California: Mayfield Publishing Company.

Cresswell, J.W. (2003). Research Design; Qualitative, Quantitative and mixed methods approaches SAGE publications.

Dimopoulos, V., Furnell, s.m., and Barlow, I.M. (2003).Considering IT Risk Analysis in Small and Medium Enterprises. Proceedings of the 1st Australian Information Security Management Conference 2003 (InfoSec03), Perth, Australia, 24 November 2003.

GoK (2007). Micro and Small Enterprises Training and Technology Project (MSETTP). Government final report.

International center for Alcohol policies ICAP (2015) Washington DC, 2015; http://www.iard.org/

Jaishankar, K (2009): Space Transition Theory of Cybercrimes. In Schamallager & Pittaro - Crimes of the Internet. Pearson Prentice Hall. New Jersey Longe, O., Ngwa, Wada, F., Mbarika, V. & Kvasny, L. (2009a).

Jaques, R. (2003). Survey finds firewall and antivirus software considered unimportant by SMEs, URL (Consulted September, 2004): http://www.frame4.com/php/printout689.html

Jelassi & Enders, (2008) Strategies for E- Commerce, United Kingdom ;Pearson Education.

Kothari, C.R.,(2004). Research Methodology; Methods and technique, New Age International.

Kothari, C.R.,(2004). Research Methodology; Methods and technique, New Age International.

Kyobe, M. (2008). Evaluating Information Security within SMEs engaged in E-commerce in South Africa. Retrieved March 08, 2010, from http://www.isbe.org.uk/Kyobe.

Lee, H. C., Palmbach, T. M., & Miller, M. T. (2001). Henry Lee’s Crime Scene Handbook. San Diego: Academic Press.

Longe O.B., Mbarika V.W., Jones .C. , Anadi .A., Wada .F. , Longe F.A. , Onifade .O.F.W. & Dada .G. (2010b).

Marjie, T. (2013) Computer Forensics and Cybercrime ; An Introduction , 3rd edition, Pearson , Colombus.

McCleland, et al (1989). Data Analysis. Harcourt Brace Jovanovich. ISBN 0-15-516765-0

Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Mugenda O.M., Mugenda A. G. (2003). Research Methods: Quantitative and Qualitative approaches, African Center for Technology Studies.

Nattaradol, P. (2002), Harnessing ICT potential for the benefits of farmers and the rural poor: Experience and vision of Bank for agricultural cooperatives (BAAC), Thailand. BAAC. URL (Consulted October, 2007):

Orford, J., Herrington, M., and Wood, E. (2004). South African Report Global Entrepreneurship Monitor. Retrieved January 22, 2005, from www.gsb.uct.ac.za/gsbwebb/userfiles/GEM_ 2004.pdf .

O'hanley, R. (2013)Information security management handbook. CRC Press; NewYork.

Patel, S. and Zaveri, J. (2010). Assessment model of cyber-attacks on information systems. Journal of computers, 15(3): 352-359

Reith, M., Carr, C. & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, Vol. 1 No. 3. Online: http://www.ijde.org/docs/02_fall_art2.html

Ridgetop Information Solutions LLC www.profhelp.com Charmayne Cullom, Ph.D. August, 2001 Attacks on organizations and individuals.

Robin L.P, (1997), Research Ethics, Cases and Materials. Indiana University Press, USA.

Rogers, M. and Kathryn C. (2012) Digital Forensics and Cyber Crime; 4th edition Pearson , Colombus USA.

Runyan, B., K. Smith, and L.M. Smith. 2008. Implications of Web Assurance Services on E-Commerce. Accounting Forum, Vol. 32: 46-61.

Saunders, M.K, Thornbill, A. (July 10 2001) Research Methods: for Business Students, Prentice Hall; 5 edition

Sony Pictures Entertainment Notice Letter (PDF). State of California Department of Justice Office of the Attorney General. December 8, 2014. Retrieved December 20,2014

Spencer, L. Ritchie, J. (2002) Quality in Qualitative Evaluation; A framework for assessing research evidence, The British academy Journal, 6:99-105

Suter, M (2007) A Generic National Framework for Critical Information Infrastructure Protection (CIIP) Center for Security Studies, ETH Zurich

Symantec Internet Security Threat Report 2014, Annual Threat report; Symantec incorporation.

United Nations Economic and Social Commission for Asia and the Pacific (UN-ESCAP)/Asian and Pacific Training Center for Information and Communication Technology for Development (UN-APCICT) and Ministry of Strategy and Finance, Republic of Korea. 2012. “Knowledge Sharing Series. Issue II. Cybersecurity.” Republic of Korea: UNAPCICT/ESCAP. Available at

Workshop Report on Effective Cybercrime Legislation in Eastern Africa

Dar Es Salaam, Tanzania, 22-24 August 2013

By Patrick Mwaita and Maureen Owor (ACCP)

Zaballos, A. and Herranz, F. (2013) From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation. Inter America development crime.

APPENDIX
Questionnaires:

The Effects of Cybercrime on E- Commerce; a model for SMEs Questionnaires

Business Name: ____

Business Background Information

1. What kind of business does the company deal in? ______________________
   ____
2. How many employees are parts of the business? _______________________
3. What is the computer primary function within the company? ____________
   ____
4. Is Internet utilized as a daily routine in the business? ___________________
   ____
5. How many computers are used within the business? ___________________
6. Does everyone work from the central office? ___________________________
7. Does everyone have the same level of access to the computer? ___________
   ____
8. Does the company have their own server? _____________________________
   ____

Business Knowledge on Security and Computers

1. What reference points does your company use for any queries on computers and security? (Please tick on the boxes)

   □ Friends
   □ IT Experts
   □ Magazine and newspaper
   □ Computer dealers
   □ Web
   □ Government security Experts
   □ Family
   □ Other companies

   Reason____
   ____

2. What triggers your system upgrades and security?

   □ Friends
   □ IT Experts
   □ Magazine and newspaper
   □ Computer dealers
   □ Web
   □ Government security Experts
   □ Family
   □ Other companies

   Reason____
   ____

Security measures in place to combat Cybercrime

1 a) what security measures / policies does your company use to prevent and eliminate Cybercrime attacks?

____

____

____

1 b) who is responsible for looking after such areas?

____

____

1 c) Do they have any experience prior to dealing with security in your company?

Y □/ N □

Reason:

____

____

1 d) How often are security issues assessed? Why?

□ Every 6 months □ Every ___ years □ Annually □ Never

Since the company started has there been an attack?

Reason:

____

____

1 e) What is assessed?

System specific controls □ Baseline controls □ Responsibilities □

Security policy □ Security awareness □ Management Process □

1 f) Are you aware of the below security measures?

i. Encrypted log in session___________________________________

ii. Password security measures____

iii. Encrypted data transfer and stored files mechanisms___________________

iv. Antiviruses and antimalware software enforced? ______________________

1 g) Is there any collaboration with other employees about security and their involvement? Y / N

2 a) Approximately how much money and resources in your company are directed specifically to Securing the computers against cyber-attacks? Why?

Reason:

____

____

2 b) Are the resources and money specifically budgeted for? Y / N

2 c) How are these estimations made? ___________________________________

<u>Explore the Amount of Attacks that SMEs are experiencing</u>

1) What experience has your company had to date with viruses, fraud, hacking and other general attacks?

How many instances? ---

What were they--

____

How did you notice it / them?

1. ---
2. ---
3. ---
4. ---

2) Did any aspect of security change after the attacks? Y / N

3) The Government is currently attempting to create a big push towards all SMEs utilizing the Internet and E-commerce as part of their daily business. Do you think that this will have any effect on the amount of security threats that you will encounter? Y / N

Reason:

____

____

Extras:

____

____