2018

# Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises

Eric Muhati
*Strathmore Business School (SBS)*
*Strathmore University*

# FACTORS AFFECTING CYBER-SECURITY IN KENYA: A CASE OF SMALL MEDIUM ENTERPRISES

**Eric Muhati**

Submitted in Partial Fulfillment of the Requirements for The Degree of Master of Business Administration.

**Strathmore Business School**

**Strathmore University, Kenya.**

**April 2018**

Declaration:

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself:

ERIC MUHATI

STUDENT NO: 052423

STRATHMORE BUSINESS SCHOOL

**Signature..... Date.....**

**Approval**

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

**Supervisor:** DR. HUMPHREY NJOGU

**Faculty Affiliation:** Strathmore University

**Signature** **.....**

**Date** **.....**

# ACKNOWLEDGEMENTS

Thankful to Jesus, my mom, my son, Dr. Njogu, Dr. Muthuma and Mr. Kibathi. Forever grateful.

# Abstract

Computer systems have translated data to be world's new basis for competitive advantage, a platform threatened by cyber-crime. With increased cyber-threats, cyber-security is no longer frivolous and requires attention from both large and small enterprises. Small Medium Enterprises (SMEs) are worse hit by cyber-crimes due to limited resources addressing emerging cyber-threats. Economics place challenges facing cyber-security into perspective better than pure technical approaches, with studies indicating cyber-security responsibilities and liabilities heavily plagued by leadership and legislation.

This study sought to explore coherent factors influencing business strategies across different SME industries trying to fix cyber-insecurity. In pursuing this goal, the study assessed economic factors considered critical for creating a safe and secure cyber-space business environment for SMEs including leadership and government policies. The researcher hopes the research results will provide better understanding of SME cyber behaviors and guide the development of appropriate solutions to SMEs cyber-space challenges.

The study is a descriptive research with surveys on components showing cyber-security factors contributing, or not contributing to reduced cyber-threat effects. Analysis was done using the statistical software-SPSS. The study targeted a 95% confidence interval for the analyzed sample. Further, a Cronbach Alpha test was used to assess reliability and correlational analysis while testing for significant relationships from data collected.



**Keywords:** cyber-security, cyber-crime, cyber-attacks, cyber-space, strategic leadership, SMEs**.**

# Table of Contents

# List of Tables

# List of Figures

# List of Abbreviations

| | |
|---|---|
| **CA** | Cyber-attacks |
| **CS** | Cyber-security |
| **SMEs** | Small and Medium Enterprises |

# Definitions

**Cyber-attacks** – Cyber-attack is defined as an unauthorized intrusion into a computer system and its related networks (Das & Nayak, 2013).

**Cyber-security** - Cyber-security is defined as a term used to generalize mechanisms designed to guard data, networks, and systems against unapproved exploitation known as Cyber-attacks (Das & Nayak, 2013)**.**

**Cyber-space** - Virtual computer world, and more specifically, an electronic medium used to form a global computer network to facilitate online communication. (Das & Nayak, 2013)**.**

**Cyber-crim**e - Cyber-crime can be defined as criminal activity(s) in which computers or computer networks are a tool, a target, or a place for criminal transactions (Das & Nayak, 2013).

**Threat actor** - also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security (Das & Nayak, 2013).

**Small and Medium Enterprises (SMEs) -** Migiro (2006) makes a distinction in the case for Kenya on the difference between a small enterprise and a medium enterprise. The author states that small enterprises are defined as businesses that have 9-49 employees, whereas medium enterprises are businesses with 49-99 employees

**Strategic leadership** - Strategic leadership refers to the capability to guide and influence others to make decisions that build on the prospect of long-term success for the business (Ahlgreen, 2010).

# Chapter 1: Introduction

## 1.1 Background information of the study

SMEs constitute 98% of businesses in Kenya, 30% of the workforce and 3% of Kenya's GDP (Mutegi, 2015). This shows the importance of secure cyber-space to SMEs who have a huge influence in the Kenyan economy. There is a myriad of challenges encountered by SMEs in ensuring a strong cyber-security response to cyber-attacks including but not limited to inadequate funds, lack of knowledgeable employees and so on. While leadership strategies are important towards these challenges, the response to large scale existential cyber-threat has often been unsynchronized and halfhearted.

To understand cyber-security without a plethora of technical terms and from a scholarly perspective, cyber-security is a term used to generalize mechanisms designed to guard data, networks, and systems against unapproved exploitation known as cyber-attacks (Das & Nayak, 2013). Cyber-attacks can cause disruptions resulting in significant reputational and financial damage to organizations no matter how resilient they may be. Despite undertaking huge resources to protect systems, countless recent successful cyber-attacks show threat actors cannot be permanently eliminated.

Global spending on cyber-security will exceed $1 trillion cumulatively over the next five years while in the same period cyber-crime is predicted to cost the world in excess of $6 trillion annually (Morgan, 2017a). Cyber-crime broadly describes criminal activity(s) in which computers or computer networks are a tool, a target, or a place for criminal transactions. An alarming fact is nearly half of all cyber-attacks are committed against SMEs (Morgan, 2017b).

Cyber-fears have percolated upwards, from the expert level to executive decision-makers (Cavelty, 2014). In order to solve the problems of growing vulnerability and increasing cyber-

crime, it is important to highlight secure cyber-space barriers, while discussing strategies helping improve cyber-security. As different strategies are implemented to try to handle the cyber-security juggernaut, many business environments seem to be facing a "security dilemma", where efforts by one actor to enhance its security, decrease the security of others (Jervis, 1978). This is because cyber-capabilities cannot be easily divulged by normal intelligence gathering activities, thus uncertainty and mistrust are on the rise. ***While cyber-security strategies are sensitive and might not be easily shared between businesses, leadership remains a big factor towards success*** (Belias & Koustelios, 2014). Leadership can be internal within the business, and external from important institutions like the government.

In 1970, the economist Milton Friedman famously articulated the statement: "The business of business is business", summarizing an argument that the only social responsibility of business is to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game (Ahlgreen, 2010). ***With cyber-security in mind, this "individual" business perspective is not proper. In fact, business leaders are currently faced with diverse competitive environments dictating deeper focus on making profits, yet it is very important to handle cyber-security as a collective effort.*** Salutary studies seeking solutions to such dilemmas are important because today, the business of business is everybody's business (Grayson, 2011).

Leadership from an internal view of an organization is attributed to business owners or authorized directors but with collaboration and the sensitive nature of cyber-security intelligence, government leadership plays an important external factor towards secure cyber-space. Government responsibility to safeguard public's civil rights and civil liberties also extends to todays' cyber-space (Jervis, 1978). Since it only takes a single infected computer to potentially infect thousands and perhaps millions of others, cyber-security is a shared responsibility with different roles played

by different parties (Das & Nayak, 2013). To unearth successful or failing cyber-security strategies among SMEs not only serves the purpose of ensuring resources are allocated to necessary channels but also, costly mistakes are highlighted and avoided.

This study sought to contribute to a better understanding of this ever-evolving cyber-threat landscape and its effect on SMEs by providing a clear picture of ***current leadership, government and cyber-security platforms strategies*** towards secure cyber-space.

## 1.2 Problem definition

Businesses, in particular SMEs that have adopted strategic cyber-security frameworks to engage in a secure cyber-space, have not fully realized the value of this undertaking with continued cyber related losses (Serianu, 2015). It is however not clear what factors and roles played by different business entities are leading halfhearted efforts by SMEs to comprehensively deal with cyber-insecurity. As long as these factors are not clearly assessed providing a solutions toward secure cyber-space, cyber-insecurity remains a real challenge particularly for SMEs given they are hardest hit by cyber-crime.

According to Symantec (2016), 43% of total cyber-attacks are aimed at SMEs, meaning they are six times more likely to become victims of cyber-crime than larger corporations. 61% of cyber-breaches hit smaller businesses in 2016, up from 53% in 2015 (Verizon, 2017)**.** Governments on the other hand are encouraging IT adoption by SME to address poverty, facilitate networking and alliances between buyers and sellers, improve market intelligence, and increase productivity (Nicol, 2003). While IT can provide such benefits, the rise in the level of electronic abuse and cyber-threats must go hand in hand with legislation and policies that provide general legal mechanisms to deal with threat actors. Indeed, the Communication Authority of Kenya in ICTA (2014), states that **no single institution has the capacity to effectively deal with cyber-threats**.

While internal factors like leadership influence the steps SMEs would take towards cyber-security, government policies and legislation are very important external success factors.

This study therefore sought to explore collective role of strategic leadership and government in addressing the challenges of cyber-threats. The study assessed factors affecting cyber-security that would guide businesses especially SMEs, in making strides towards achieving true value in securing cyber-resources.

## 1.3 Research Objectives

The general objective of this study is to seek an effective solution that recognizes the role played by strategic leadership, government policies and cyber-security product engineers in enhancing cyber-security adoption by SMEs.

*Specific objectives are:*

I. To assess strategic leadership factors influencing cyber-security adoption by SMEs (Internal factors).
II. To assess government policies influencing cyber-security adoption by SMEs (External factors).

## 1.4 Research Questions

1. How are SME leaders in Kenya strategically tackling increased cyber-threats and cyber-attacks?
2. What role is the government of Kenya playing to improve secure cyber-space for SMEs?

## 1.5 Scope of Study

The study looked at leadership strategies of those at the helm of SMEs in Kenya. The study sought to investigate ways of increased collaboration between cyber-security stakeholders and

SMEs. The study is also central to the familiarization of all SMEs staff on cyber-security matters because in many cases they are the direct targets of threat actors (hackers). More so, the study focused on engagement of SMEs leaders with the other key stakeholders, including the government, in the cyber-security sector and how they can commit to ensuring a safer cyber-space for SMEs.

## 1.6 Significance/Justification

This research will contribute to knowledge on how SME leaders can engage more with other cyber-security stakeholders including government, to ensure Kenya's SME cyber-space protection is enhanced. The study will ensure interpretations of the research recommendations following the findings; can be generalized to the whole SMEs population in Kenya, and reward with recognition, best cyber-security adoption practices.

## 1.7 Conclusion

Technology has had an unprecedented growth and is often lauded as a critical catalyst for business development in modern society. On the other hand, cyber-crime with its complexities has proven difficult to combat due to its esoteric nature. Thus, the question whether technology is helping SMEs overcome their disadvantages and contributing to their overall growth and performance becomes important (Michiels & Crowder, 2001). There might not be one measure to cure the menace of cyber-crime and ensure cyber-safety but a combination of measures together might reduce risks most effectively and efficiently.

# Chapter 2: Literature Review

## 2.1 Introduction

One major reason for reviewing literature is to help researchers generate and refine research ideas (Saunders, Lewis, & Thornhill, 2009). This chapter sought to analyze relevant literature regarding factors affecting cyber-security strategies by Kenyan SMEs through analyzing literature that supports the study (theoretical literature) and statistics or facts that show importance of the study (empirical literature). The review highlights existing literature gaps that should be addressed then shows the conceptual framework. The literature was reviewed in two categories, theoretical and empirical frameworks.

## 2.2 Theoretical Framework

Theoretical framework serves as a basis for conducting research, determining points of measure and what relationships to look for. Rowe (2014) suggests theoretical classification along literature goals with respect to theory (describing, understanding or explaining), breadth (confined problem vs. discipline), systematic (inclusion criteria and quality assessment) and argumentative strategy. This study adopted the following for research: social-technical theory, routine activity theory and rational choice theory.

### 2.2.1 Description, understanding, and explanation

#### *2.2.1.1 Socio-technical theory*

Social-technical theory hypothesizes the presence of two sub-systems in every organization or corporate; these are technical and social sub-systems (Cartelli, 2007**)**. The technical sub-system can be identified with processes responsible for converting system inputs into system outputs i.e. business equipment. On the other hand, the social sub-system is much more than the set of technical control tasks performed by people. Technical tasks are combined with individual jobs

and responsibilities then assigned to groups. Social sub-systems enhance or reduce the quality of production from technical sub-systems, thus optimizing this interdependency is important in achieving maximum performance (Cartelli, 2007). The social sub-system is the environment where cyber-crime takes places since it involves human activities.

#### *2.2.1.2 Routine activities theory*

Barkan (2006) explains how the social sub-system activities fall into routine activities theory and assumes individuals will commit a crime if there is a motivated offender, a suitable target, and the absence of guardians capable of preventing an offense from being successfully committed. The theory argues that crime is normal and depends on the opportunities available. If a target is not protected enough, and if the reward is worth it, crime will happen. The internet breaks physical location barriers and provides anonymity to cyber-attackers making cyber-crime suitable. The theory is relevant to this study in that it provides significant understanding to why people engage in cyber-crime. SMEs vulnerabilities lacking capable defense against cyber-threats, coupled with routine activities theory delineates key insights on increased cyber-attacks to SMEs.

#### *2.2.1.3 Rational choice theory*

These key insights include ways of mitigating cyber-threats through rational choice theory, that considers individuals will freely choose to commit a crime after weighing prospective rewards against potential risks (Barkan, 2006). Rational choice explicitly assumes a rational offender and emphasizes the criminal's benefit and motivation but Mandelcorn, Modarres & Mosleh (2013) give another key insight to this study by recognizing the imperfect nature of decision-making from a rational cyber-defender. Mandelcorn et al. (2013) describe a major difference SMEs with limited resources face in that, cyber-attacker's skills are directed on exploiting a single SME vulnerability, but a defender has to guard against all perceived possible vulnerabilities.

Businesses today are faced with choices on how to defend themselves from potential cyber-attacks. The range and scope of these unknown attacks create the need for business leaders to prioritize their defense choices. When a leader is making decisions regarding the defense of their network, they generally have to consider the impact that defense has on business. This theory is important to this study in analyzing the impact of SME leaders' and government choices with regards to cyber-security. Cyber-criminals could be deterred if risks were certain and the punishment was severe.

## 2.3. Empirical Framework

### 2.3.1 Business enterprises – Threats faced by leaders in modern enterprises

Cyber-space is growing at a speed unprecedented by many. Almost three billion people are now connected to the Internet; a figure growing rapidly and estimated to reach five billion people, using fifty billion devices, by 2020 (Evans, 2011). As the world moves towards full connectivity also known as the "Internet of Things", extreme increase in cyber-threats has been triggered hence increased research interest. Developing countries like Kenya, are dominated by SMEs that represent between 96 and 99 percent of total enterprises. These SMEs have been observed to be most vulnerable in instances of cyber-insecurity (Serianu, 2016).

### 2.3.2 Efforts by government in addressing cyber-crime

Migiro (2006) makes a distinction in the case for Kenya on the difference between a small enterprise and a medium enterprise. The author states that small enterprises are defined as businesses that have 9-49 employees, whereas medium enterprises are businesses with 49-99 employees. In this study both categories shall be looked into.

Despite various efforts to check cyber-insecurity through a regulatory framework, things seem not to have subsided. Indeed, the African financial sector involving both large corporations

and SME players have been major targets of cyber-crime due to increased uptake of financial technology. In 2016, more than $2 billion was lost by countries in Africa because of Cyber-attacks (Serianu, 2016). The Micro and Small Enterprises Bill (MSE 2011) was specifically drafted to address issues of legislation and encourage development of this sector.

Such rife perplexity reveals that there are joint and individual leadership strategies gaps SMEs are lacking to take on the big battalions of cyber-criminals in the cyber-security domain. The focus of this study was to explore such strategies or lack of them.

### 2.3.3 Realities of Cyber-threats to SMEs

Cyber-security is concerned with the creation of safe cyberspace. According to Olayemi (2014), cyber-security issues that typically arise comprise of information secrecy, network survivability, and system's integrity. The major goal of information security (IS) is to guarantee ready dependable structures for all likelihood of cyber-related crimes and attacks. In order to accomplish day to day jobs, SMEs have to rely more on advanced technological which unfortunately comes with increased targeted cyber-attacks.

Cyber-related crimes and cyber-attacks are part of the fastest-growing activities of criminal nature in the today's contemporary world (Das & Nayak, 2013). The main concern for Das et al. (2013) is not the high increase in cyber-crime but its potential disturbance to the society, noting a positive correlation between the growth in cyber-crime incidents and the increase in computer literacy. As more businesses grow in technology uptake, a positive correlation is observed showing corresponding continuous rise in cyber-crimes. Das et al. (2013) show different industries fall victim to cyber-crime but with different degrees of economic impact. This variation in the economic impact of attacks is significant on SMEs since they face cyber-threats with fewer resources and accept risks related to exposure. While Das et al. (2013) offer an explanation for the

history and rise of cyber-security with a greater concern to SMEs, strategies to be taken by important business players in response are not addressed.

### 2.3.4 Effects of cyber-breach to SMEs

Out of the SMEs that have had a cyber-breach, 93% experienced severe impacts to their business while 60% closed businesses within six months (KPMG, 2016)**.** Large organizations have a realistic appreciation for cyber-threats they may face at one point or the other, but a lot of SMEs are usually undecided about their perceived vulnerabilities (Chak, 2015). The distinctive digital cultures in Kenya have facilitated increased mobile banking remittance thus presenting opportunities for cyber-attacks on banking institutions that facilitate these transfers. (Goodman & Traynor, 2013). While mobile banking might aid business transactions for SMEs, the apparent risks might have a different impact for large businesses who might have many ways of receiving or making payments, compared to SMEs who might be heavily relying on mobile banking.

SMEs need a strong reputation to become long-lasting companies (Abimbola & Vallaster, 2007)**,** however with successful cyber-breach KPMG (2016) defined reputation damage as the loss of clients, the ability to attract new employees and the ability to win new business and shows SMEs who suffered from cyber-breaches have damaged their reputation by 31%. The most common target for cyber-attacks is sources of liquidity. SMEs are facing a huge increase in the amount of money stolen from their bank account caused by cyber-attacks in recent years. According to the National Small Business Association (NSBA, 2014) (NSBA, 2015), the average amount stolen from an SME bank account increased from about $6,900 in 2013 to about $32,000 in 2015, representing a 462% increase. The value of the digital economy is predicted to face a high drop due to imminent cyber-attacks on businesses (Morgan, 2016). Yet this negative future is not

deterring SMEs and makes one wonder why Matambalya and Wolf (2011), finds SMEs relying much more on technology than larger enterprises.

### 2.3.5 Why SMEs Leaders contribute to increased vulnerabilities

Cisco Annual Security Report (Cisco, 2017) attempts to give an answer stating a common fallacy among SMEs is they assume they cannot be targeted by hackers because they are generally smaller in size as compared to large businesses. SME leaders perceive their businesses somehow immune to cyber-attacks and data losses. Cisco (2017) reports that organizations which have not yet suffered a security breach may believe their networks are safe. This confidence is probably misplaced, considering 49% of security professionals say their organizations have had to manage public scrutiny following a security breach (Cisco, 2017). While businesses are reacting to cyber-attacks, having proactive sensitization and appreciation of cyber-security would help increase safer cyber-space.

### 2.3.6 Strategic Leadership and Cyber-security

As with all business plans, when setting priorities, assigning tasks, implementing and monitoring cyber-security measures, it should be clear where to allocate funds and measure return on investment. Kimwele et al. (2005) address challenges faced by SMEs especially in Kenya, by providing a cost-effective framework when implementing security measures. The objective of the framework was to provide a way of tackling cyber-security challenges faced by Kenyan SMEs. They state that SME leaders should have specific roles in regards to cyber-security indicate measurable performance indicators that can help enhance cyber-security strategies, and evaluation metrics that will facilitate frequent reviews of cyber-security plans as attacks continue to evolve. This study goes a long way to articulate the challenges SMEs face when implementing cyber-security and how to approach such difficulties but fails to highlight what happens after

implementation. Do SMEs actually get beyond the challenges into post implementation? If yes, are their strategies working or not?

Matambalya and Wolf (2001) provide an overview of East Africa and specifically Kenya's situation regarding cyber-security and cyber-space. Cyber-security threats towards SMEs in Kenya and Tanzania are increasing at an alarming rate and in most cases, these cyber-crimes are not visible, thus criminals get away without prosecution. Information economies of scale where information about cyber-attacks is shared through best practices would help in the best use of technology recommendations through improved SME networks (SMEs associations sharing cyber-security intelligence), to reduce cybercrime costs. Also, Matambalya and Wolf (2001) state that as computer literate personnel is relatively scarce in both countries and enterprises have to train employees first, it is not surprising that productivity goes down first after investment in more expensive ICT systems. This, in turn, relates why cyber-security measures, if complex, are not implemented by SMEs.

### 2.3.7 Technical solutions to cyber-crime

Apart from cost, 67.3% of SMEs in Kenya identify the dearth of computer skills as a key problem in moving forward with technology in their businesses, thus they are not sure which cyber-security strategies to adopt (Migiro, 2006). While SMEs consider the internet and e-Commerce important to business, high cost, limited funds and lack of technical know-how influence the adoption of technology. Migiro (2006) suggests these issues can be mitigated through the production of convenient and efficient technology products, coupled with training and awareness creation programs. This contributes to the purpose of exploring factors considered by SME leaders in respect to cyber-security, by suggesting cyber-space players like the government should consider strategies like training and awareness before production of cyber-security policies.

Barton, Tejay, Lane, and Terrell (2016) investigate how senior management is motivated to commit to IS security. Although senior management commitment alone does not guarantee effective risk management, it is a prerequisite for better business development, implementation, and compliance with IS security controls. Effective IS security management is not a standalone activity but should be found on a well-developed security strategy. Barton et al. (2016) were seeking to comprehend what external motivators of senior managers are a crucial ingredient for the success of IS security. A correlation was not found between normative influences and senior management belief, normative influences and senior management participation, coercive influences and senior management participation. Normative and coercive motivators include alleged government domination, industry, formal education, and media coverage.

Barton et al. (2016) show that IS security-related mimetic (mimicking businesses alleged to be very successful) influences, have a greater impact on senior leaders of SMEs, giving a glimpse of uncommon probable driving forces behind investing in cyber-security. The authors suggest that many SMEs do not have the belief that they are crucial targets of cyber-attacks but take security opportunities motivated by competitors reaping benefits of cyber-security approaches. For example, having cloud-based information systems for better security since a particular SME has at least one authority reference, they have faith in and trust for cyber-security aping.

In conclusion, all literature agrees the digital era has been accompanied by fast-rising cyber-attacks activities. The major reason why the SMEs are facing bigger and bigger threats daily is that they are not investing enough in cyber-security backed by the notion that they are not cyber-crime targets. Also, it is not clear what strategic directives SME leaders are implementing to ensure their businesses systems are securer. The literature lacks content about roles of important players

like government and security engineers in providing safe cyberspace. While there is information about SMEs financial success and technology uptake, there are no highlights of successful cyber-strategic leadership actions among SMEs in Kenya. We aimed to undertake an analysis of the latter in this study.

## 2.4 Conceptual Framework

As we can see from figure 2.1 the conceptual framework consists of cyber-security dependent variables strategic leadership and government cyber-policies. Independent variable for this study include technical competency, digital culture for SME leaders, government role in protecting information infrastructure and prosecution of cyber-criminals.

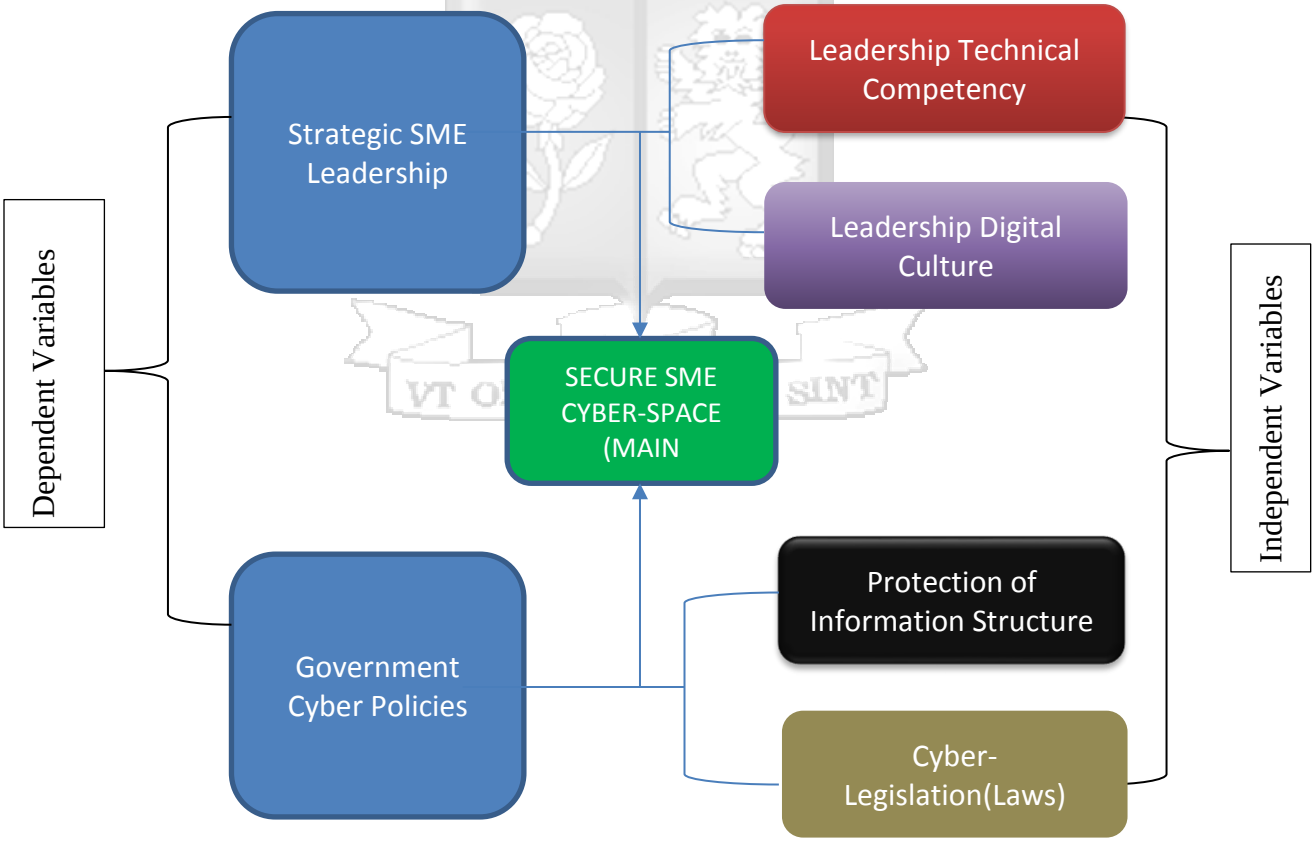


*Figure 2:1 Conceptual Framework*

# Chapter 3: Research Methodology

This chapter will primarily discuss the research design employed to comprehensively address the research problem and by extension the research objectives. The chapter highlights the population under consideration, the sample size and data collection methods.

## 3.1 Research Design

This proposed study applied a quantitative survey methodology using self-administered survey questionnaires to collect data from a sample of SMEs in Kenya. According to Amaratunga, Baldry, Sarshar, & Newton (2002) quantitative methods assist researchers to establish statistical evidence on the strengths of relationships between both exogenous and endogenous constructs. They also argued that statistical results provide directions of relationships when combined with theory and literature. Furthermore, Cavana, Delahaye, & Sekaran (2001) suggest quantitative methods can be utilized to verify the hypotheses and provide strong reliability and validity.

This is a descriptive research with surveys on components showing crucial actions steps, if any, taken by leaders dealing with cyber-threats. A mixed research approach was needed for adequate insight and knowledge into solving and achieving the research problem and objectives. The study approached the issue of cyber-security from a theoretical and investigative point of views as well as combination of existing literature studies, direct in-depth primary research and secondary materials i.e. from the internet. This assisted the researcher in the midst of existing many cyber-security aspects, yet disclosing cyber-information was not readily available.

## 3.3 Population and sampling

Representative samples ensure the opinions of one subset of the population (those who are over-represented) are not inaccurately magnified while ignoring or under-reporting the opinions of another subset (those who are under-represented, or not represented at all) but a close

equilibrium is achieved (Redmiles, Acar, Fahl, & Mazurek, 2017). This study was opened to a widespread SME society. The survey determined if respondents are from an SME business making a correlation between business sizes and economic sector. The total population was 1,338, 480 and the sectors included wholesale and retail trade; repair of motor vehicles and motorcycles, manufacturing, accommodation and food service activities and lastly, other service activities. The study adopted the following sampling methods:

### 3.3.1 Sampling method

A larger sample size usually involves more expenditure on collecting and analyzing of data (Henry, 1990). Therefore, this research balanced the trade-off of getting a satisfactory sample size within budget and time constraints. The sampling frame for this study was created based on different sectors so long as the organization is a Licensed SME. Unlicensed SMEs were not considered as it was hard to reach them due to lack of licensing contact information on registered leaders/business owners. Roscoe (1975) suggests sample sizes larger than 30 and less than 500 are appropriate for most research. Given that this study specifically targeted licensed SMEs due to time and research constraints and only half of the sample size generated was considered.

According to figure 4.2 Kenya National Bureau of Statistics (2016), the SME space can be broadly classified into licensed and unlicensed with major sectors that have more than 5% economic activities being 57.1% (licensed) and 62.9% (unlicensed) in wholesale and retail trade; repair of motor vehicles and motorcycles, 11.2% (licensed) and 12.0 (unlicensed) in manufacturing, 8.8% (licensed) and 9.1 (unlicensed) in accommodation and food service activities, and 8.7 (licensed) and 5.4 (unlicensed) in other service activities. These are the sectors considered in this study.

Total licensed SMEs in sectors having more than 5% economic activities is 1,338,480. Using the Cochran's formula assuming half the population gives maximum variability (0.5) and a confidence level of 95% that gives us Z values of 1.96, per the normal tables, we get

$$n_o = \frac{Z^2 pq}{e^2} \quad \text{hence } n = \frac{1.96^2 \text{ X } 0.5(1-0.5)}{0.05^2} = 384$$

Due to brevity this study considered at least half the sample size of 384. Indeed, this sample size calculation estimate is confirmed by Saunders et al. (2009, pg. 219) as their pre-calculated sample size.

## 3.4 Data Collection methods

Questionnaires were administered online with awareness created through social media platforms. 3 prominent personalities on Facebook and Twitter, who have more than 10,000 followers, shared a link asking for voluntary respondents as can be seen in figure 3.1. Other questionnaires were distributed and information collected by research assistants. The researchers contacted SME leaders requesting them to participate in the survey. Those who responded positively were then emailed the online questionnaire link. In some cases, the questionnaires were delivered physically by the research assistants and picked up on completion. The respondents were assured that all personal information would remain strictly confidential.

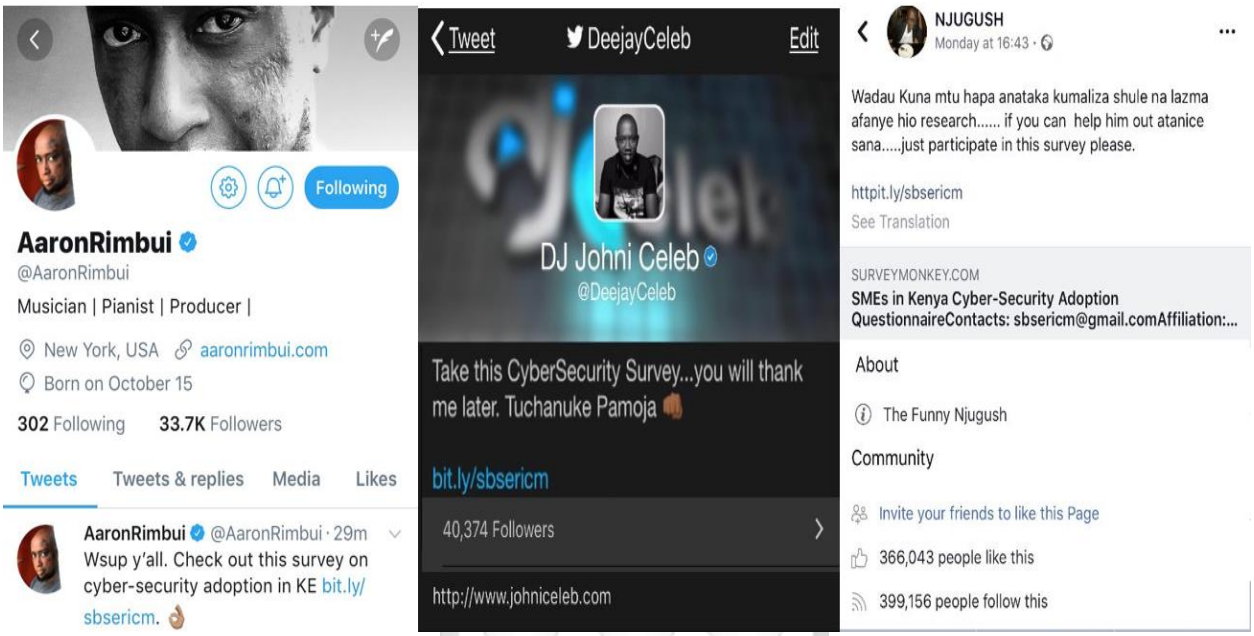


*Figure 3:1 Crowd Sampling*

## 3.5 Data analysis

According to Shamoo and Resnik (2003), various analytic procedures provide a way of drawing inductive inferences from data and distinguishing the signal (the phenomenon of interest) from the noise (statistical fluctuations) present in the data. This study was concerned with understanding strategies against cyber-attacks and the 4 major SME sectors covered in 5 dimensions with close-ended statement representing each dimension. The responses were assessed on a five-point Likert scale whereby 1 represented "strongly agree" and 5 "strongly disagree". Responses were checked based on true or false data management done by using Microsoft Excel sheet and statistical package (SPSS, ver. 20).

### 3.5.1 Descriptive statistics

Descriptive statistics was applied to investigate and describe characteristics of technical management practices of SMEs in the sample, with a special focus on cyber-defense strategies. This included calculation of averages, frequency distribution, and percentage distribution used as

a form of summarizing data. Cross-tabulation was used to inspect differences and to make comparisons between two groups of SMEs, with and without efficient cyber-security leadership strategies.

### 3.5.2 Inferential statistics

Inferential statistics is the method used to draw conclusions about the population itself. While the descriptive analysis allows the researcher to generalize from the sample to the population; inferential statistics allows the research to draw conclusions about the population on the basis of data obtained from samples (Blanche, Durrheim, & Painter, 2006). This was important as it helped apply findings to sectors not represented in the selected sample population like the financial sector which is a crucial sector, to draw conclusions based on selected sectors.

### 3.5.3 Multivariate analysis

Profitability is inherently multidimensional. It can be simultaneously influenced by many dimensions. In terms of management, profitability can be influenced by the efficiency of cyber-security management, marketing management, financial management, production management, and systems quality management. By assuming other things held equal, this study concentrated on examining the effect of cyber-security management on SME profitability. Even though this assumption is held, the effect of cyber-security management on SME profitability still has a multidimensional characteristic since profitability can be influenced by business industries or even new legal policies. When problems are multidimensional and three or more are involved, we utilize multivariate analysis. Multivariate statistical methods allowed the effects of more than one variable to be considered at one time (Zikmund, 1997, p. 656).

## 3.6 Research Quality - validity, reliability, and objectivity of the research

### 3.6.1 Validity and reliability

Data was presented without any sophistry. To avoid inconsistencies and deviations, participants were asked to go through the questionnaire once when the survey was finished, to add something if they considered it important or to correct themselves if they think they did not understand some question well. This was done for the purpose of ensuring validity of collected data. The research was subjected to a reliability test to check for consistency with work done by others and this study. There are three types of validity tests namely content, construct and criterion-related validity tests (Zikmund, 1997). Content measures the degree to which the content of the items adequately represents the universe of all relevant items under study. Criterion-related measures degree to which the predictors are adequate in capturing relevant aspects of the criterion. Construct identifies the underlying constructs being measured and determine how well the tests represents them (Zikmund, 1997). The study involved pilot questionnaires sent to a 20-member focus group for evaluation of validity ratio as recommended by Kothari (2004) who states 5% to 10% of the sample can be adequate for running validity and reliability tests. Tests of reliability aim to show if findings can be relied upon to provide the same values if the survey questionnaires were to be administered repeatedly under similar conditions. The results obtained from the 20 questionnaires were entered into SPSS and Cronbach reliability test performed. A coefficient above 0.7 is recommended for general studies while that above 0.8 is recommended for clinical studies (Kurpius & Stafford, 2006). This study used Cronbach's alpha reliability coefficient of 0.7 since it's not a clinical study.

### 3.6.2 Objectivity

Cyber-security being the major subject under research provides some participation bias where data collection is concerned. This might occur when a certain group of participants are more or less likely to participate than others, like in cases between those who've experienced or not experienced successful cyber-attacks.

### 3.6.3 Ethical Issues

The topic of research deals with security and demands high ethical practices. Data must remain confidential. Ethical standards were deployed without any hidden conditions and all privacy of issues was clarified. Informed consent was sought from each individual before conducting the study in a manner that guaranteed the safety and privacy of each respondent i.e. no release of system's security vulnerabilities. To ensure confidentiality, critical details were encrypted through transposition cipher and stored in password enabled Microsoft Excel files. Consent and approval for the study was sought from Strathmore ethical and review board (Appendix 4).

# Chapter 4: Presentation of Research Findings

Guided by the research objectives and questions, the study collected data to assess both dependent and independent variables factors affecting secure cyber-space for SMEs through available respondents' knowledge. This chapter presents findings based on background information of respondents, dependent/independent variables and study objectives.

## 4.1 Preliminary study results

### 4.1.1 General Findings

#### *4.1.1.1 Response Rate*

The questionnaires were administered both physically and online. The online platform was set not to allow multiple entries from a particular device. Later on, after the survey was closed, the platform was set to allow multiple entries as physical questionnaires were imported into the survey collector database. 250 physical questionnaires were printed with 197 returned fully filled, whereas online questionnaires started totaled 103 with 62 successful completions. Denscombe (2014) states a response rate of 60% is acceptable and can be considered for analysis. Referring to figure 4.1 we see the study has an acceptable 73% response rate.

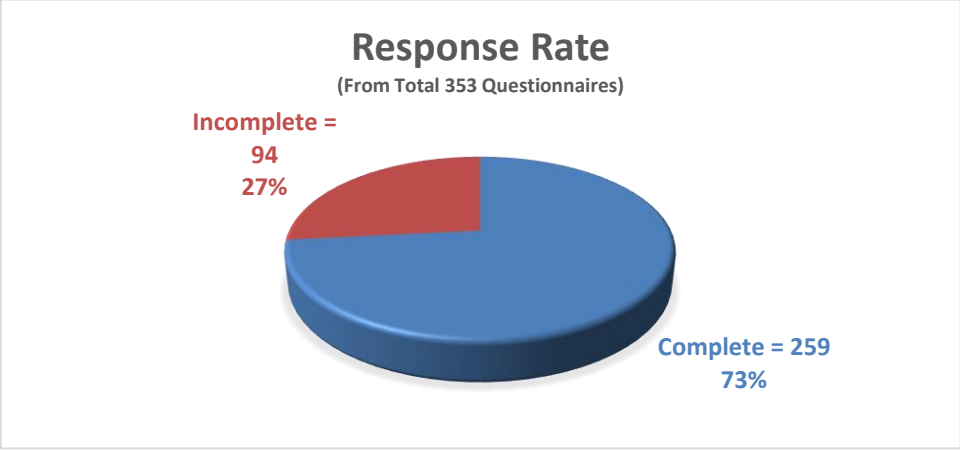


*Figure 4:1: Questionnaire Response Rate*

#### *4.1.1.2 SME Industry Sector*

To be able to apply the results of the findings across different SME sectors it was important to understand which sector the respondent belonged to. Majority (41%) SMEs belonged to Wholesale/Retail-trade/Repair-of-Motor-Vehicles/Motorcycles. Manufacturing had the least (6%) respondents as seen in figure 4.2.

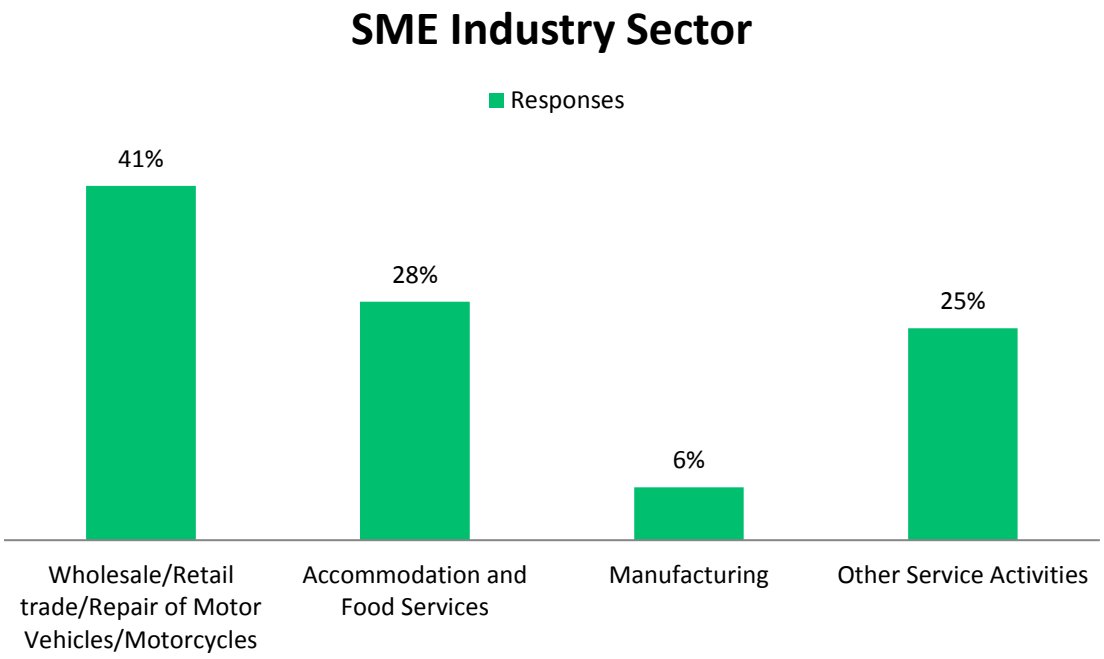


*Figure 4:2 SME Industry Sector*



### 4.1.2 Findings on Objective 1 (Leadership factors)

#### *4.1.2.1 Approximate Annual Turnover*

In regards to objective 1 and the independent variable leadership digital culture, the study established the SME annual income. The study was dominated by SMEs having between 500,000 and 5 Million (43%) annual turnover likely due to accessibility compared to SMEs with more than 100 Million (6%). The annual turnover will be important when understanding cyber-security budget in section 5 on discussions.

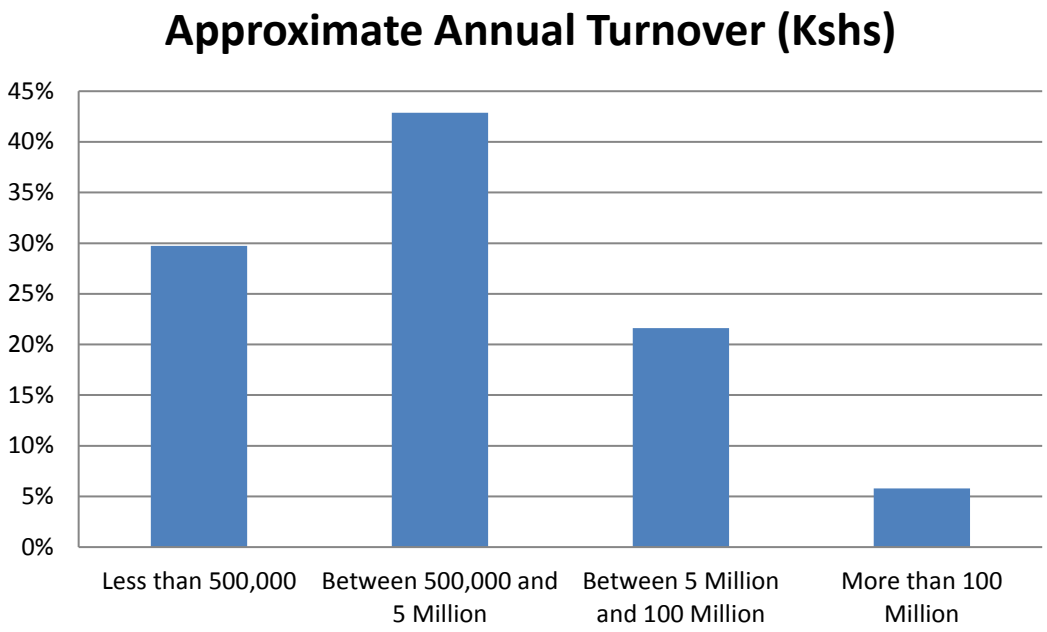


*Figure 4:3 Approximate Annual Turnover*

### *4.1.2.2 Interdisciplinary Job Functions*

To understand leadership technical competence in objective 1, the study sought to understand cross-cutting job functions of the respondents. Referring to figure 4.4, the study found 25% of the respondents believed they had some general management responsibilities. IT also ranked high (24%) probably due to the integral role of technology in business operations. The least represented interdisciplinary job function was finance and accounting (4%) most likely from its specialty and sensitivity of monetary resources. It is also important to note the study found from most respondents that business process automation (74%) and information management (67%) were the major core issues covered on cyber-security implemented strategies but very little consideration was given to legal compliance (17%) as figure 4.5 shows

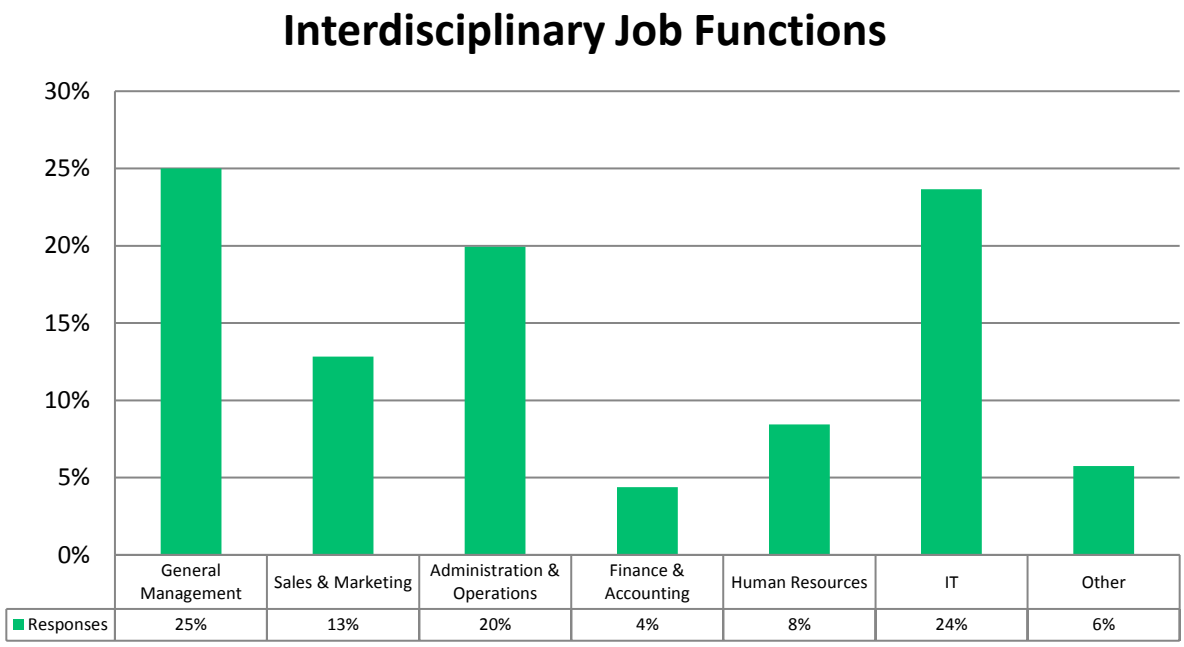


*Figure 4:4 Interdisciplinary Job Functions*

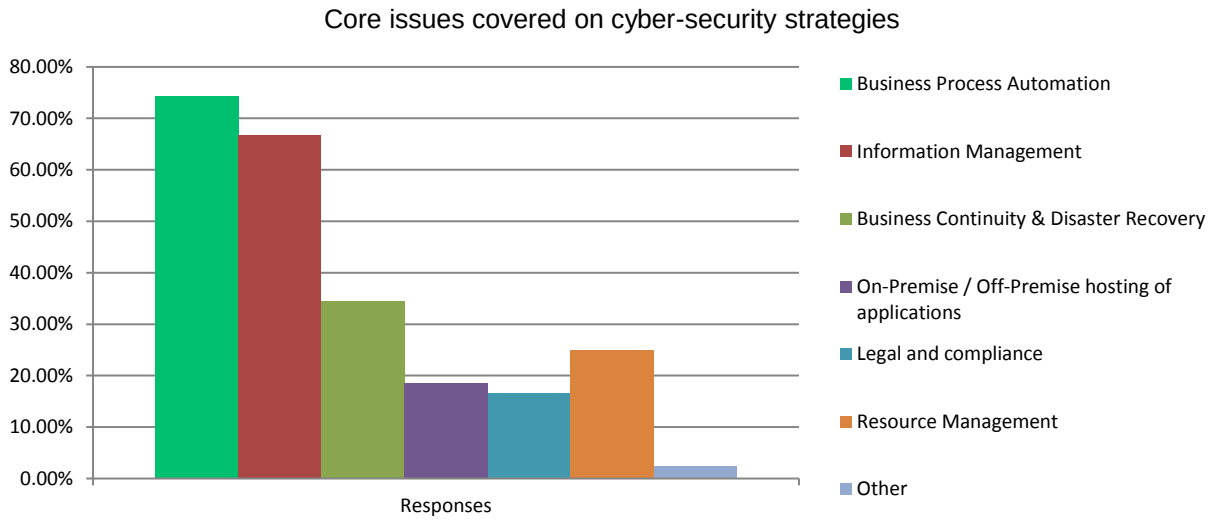


*Figure 4:5 Cyber-security core issues covered*

### *4.1.2.3 Leadership Cyber-Security Strategies Vs Preparedness for Cyber-threats*

Objective 1 of the study concerned with leadership technical competence resulted in findings as figure 4.6 shows. It's abstruse to find majority of the respondents (62% + 10%) not

confident of their cyber-security technology strategies yet, 83% believed were confident of their preparation for cyber-attacks.

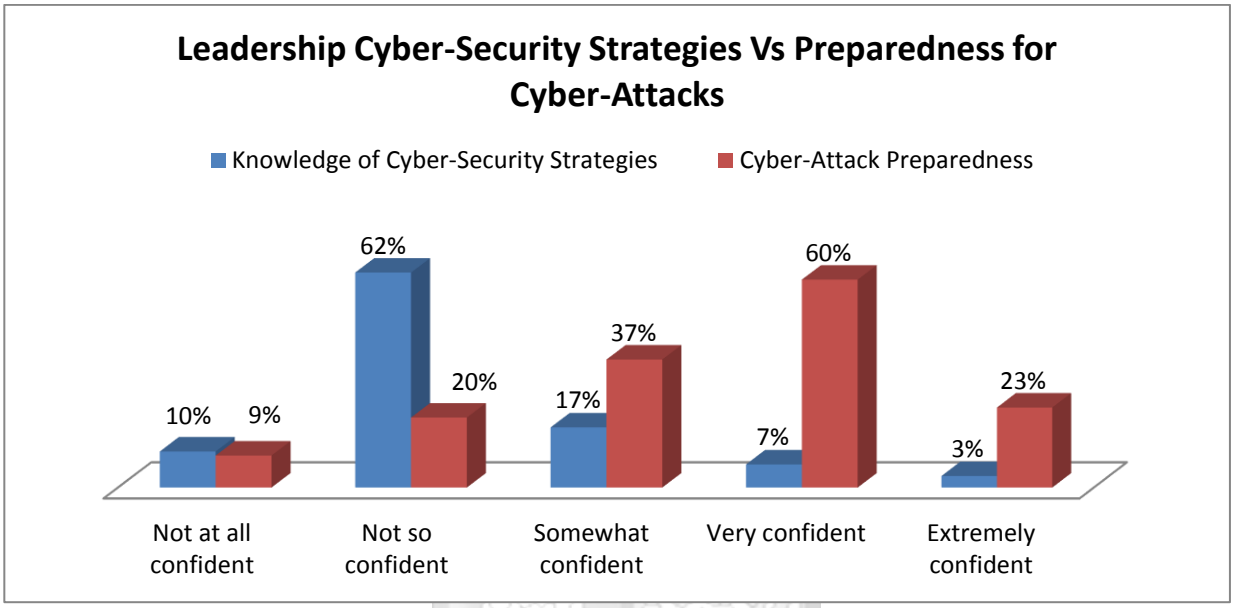


*Figure 4:6 Leadership Cyber-Security Strategies Vs Preparedness for Cyber-Attacks*

### *4.1.2.4 Recent cyber-security activities*

For objective 1, the study sought to understand SMEs who had recently deployed cyber-measure in order to identify how independent variable of leadership digital culture affected provision of secure cyber-space. Only 17% of the respondents had not recently deployed measures towards cyber-security as we can see in figure 4.7 basically due to lack of finances (41%) as per figure 4.8.

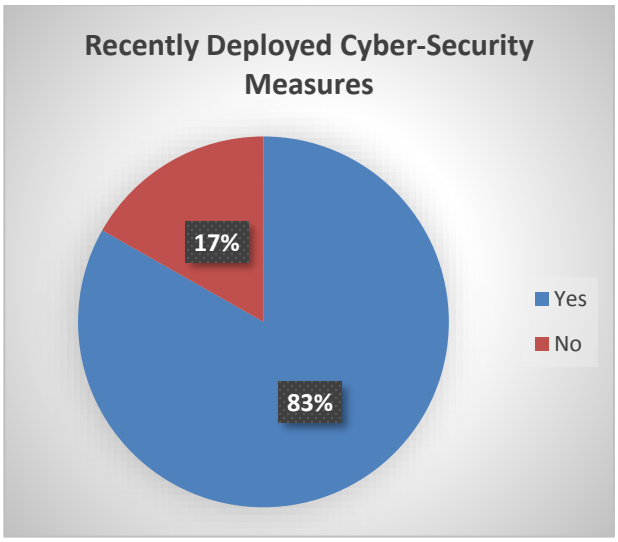


*Figure 4:7 Recent cyber-security measures*

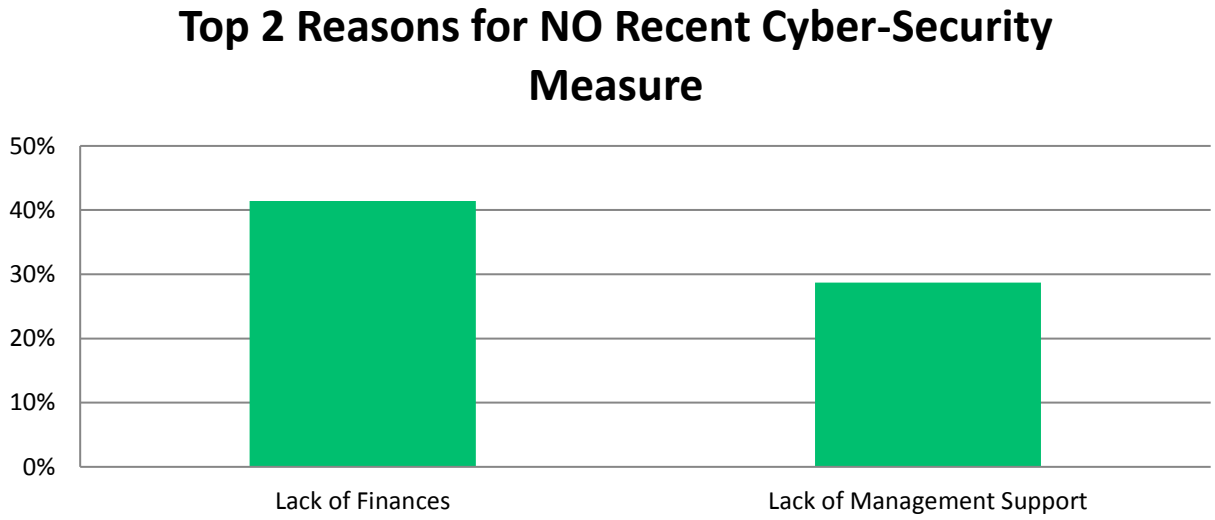


*Figure 4:8 Reason for NO recent cyber-security measure*

At the same time referring to figure 4.9, the study found respondents who've recently deployed cyber-security measures mostly covered email and communication (70%) most likely due to rampant communication interceptions and hacks.

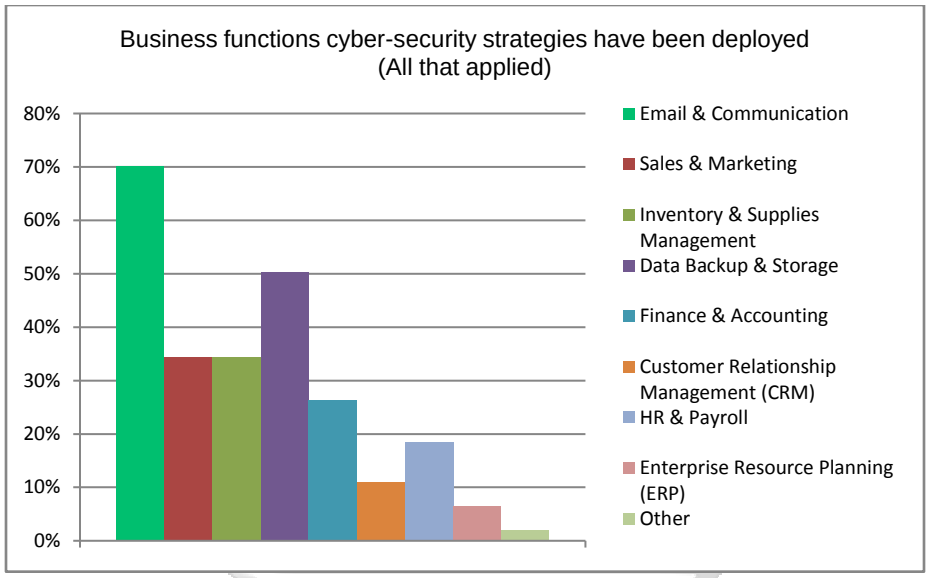


*Figure 4:9 Business functions cyber-security strategies have been deployed*

### *4.1.2.5 Factors determining cyber-technology choice*

In terms of leadership digital culture related to objective 1, for 216 respondents (83% of total 259) with recent cyber-security undertakings as we can see in figure 4.10, the study established flexible cost (71%) as a major reason that would influence leadership digital culture where cyber-security is concerned.

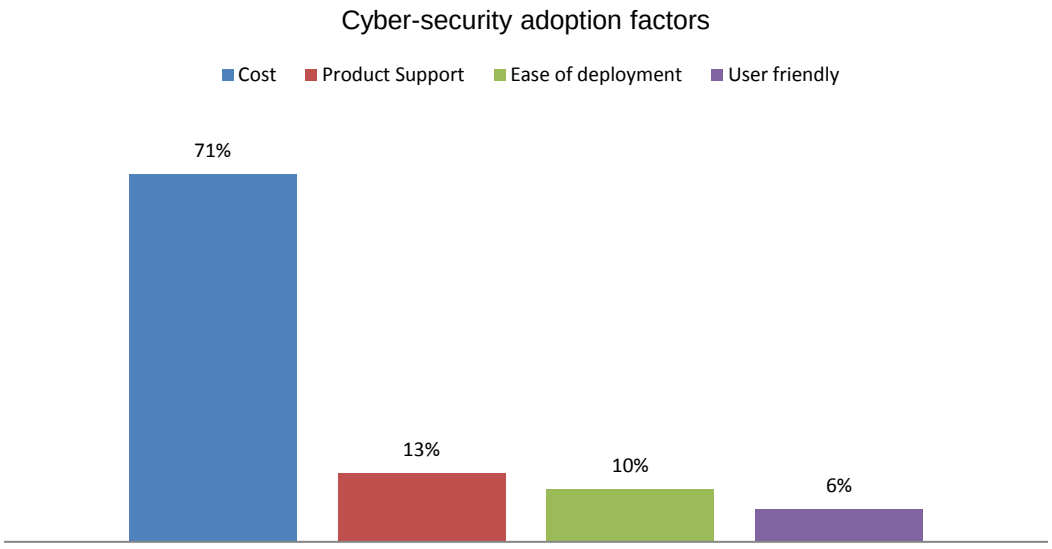


*Figure 4:10 Cyber-security adoption factors*

#### *4.1.2.6 Cyber-security technical skills available*

For objective 1 understanding leadership technical competence, table 4.1 below summaries skills available in 216 businesses with recent cyber-security measures. Relevant diploma in cyber-security leads with 108 and relevant master's degree recording least number (20) probably due to education costs.

*Table 4:1 Cyber-Security Skills*

| Cyber-Security Skills | Number |
|---|---|
| Professional Certificate in Cyber-Security | 15 |
| Relevant Bachelor's Degree in Cyber-Security | 36 |
| Relevant Master's Degree in Cyber-Security | 20 |
| Relevant Diploma in Cyber-Security | 108 |
| Relevant Outsourced Contracts | 37 |
| **Total** | **216** |

### 4.1.3 Findings for Objective 2 (government factors)

#### *4.1.3.1 Knowledge on cyber-security related legislation*

For objective 2 on government factors SME secure cyber-space, most respondents (66%) are not familiar with any cyber-security laws or cyber-crime penalties as we can see on figure 4.11 while in figure 4.12, 50% of the respondents believe utmost urgency in cyber-security legislation is required to improve SMEs business space.

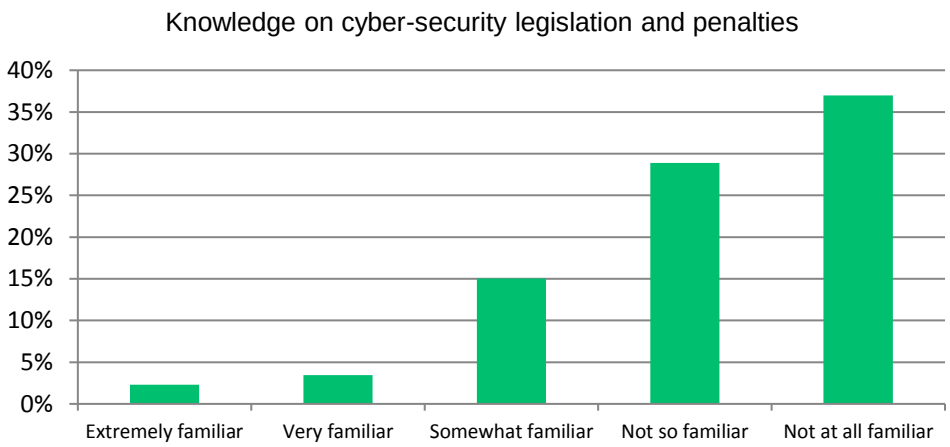


*Figure 4:11 Knowledge on cyber-security legislation and penalties*

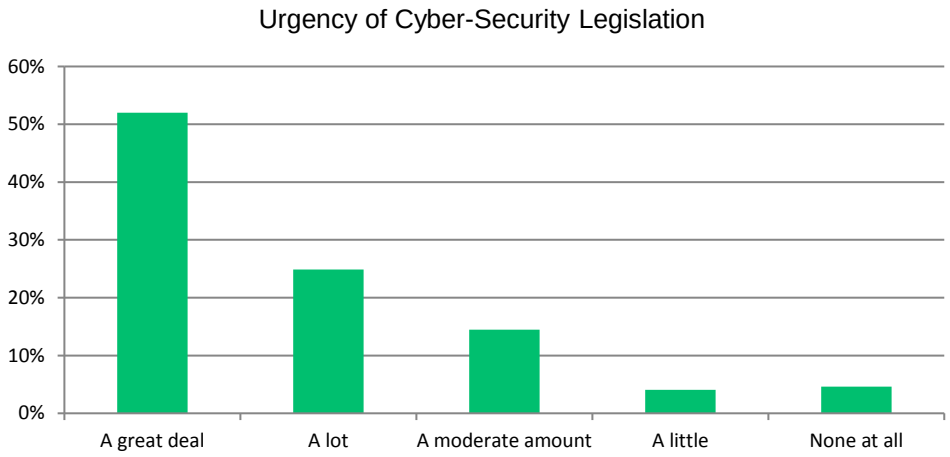


*Figure 4:12 Urgency of Cyber-Security Legislation*

### *4.1.3.2 Government cyber-security initiatives.*

As we can see in figure 4.13, over 80% of the respondents were not aware of any anti-cyber-crime government teams or any cyber-security roadmaps, but 40% were aware of internationally recognized cyber security standards against cyber-crime. The study also found most respondents do not value current Government cyber-security initiatives and actually 63% rate higher education initiatives are very deficient as per figure 4.14.

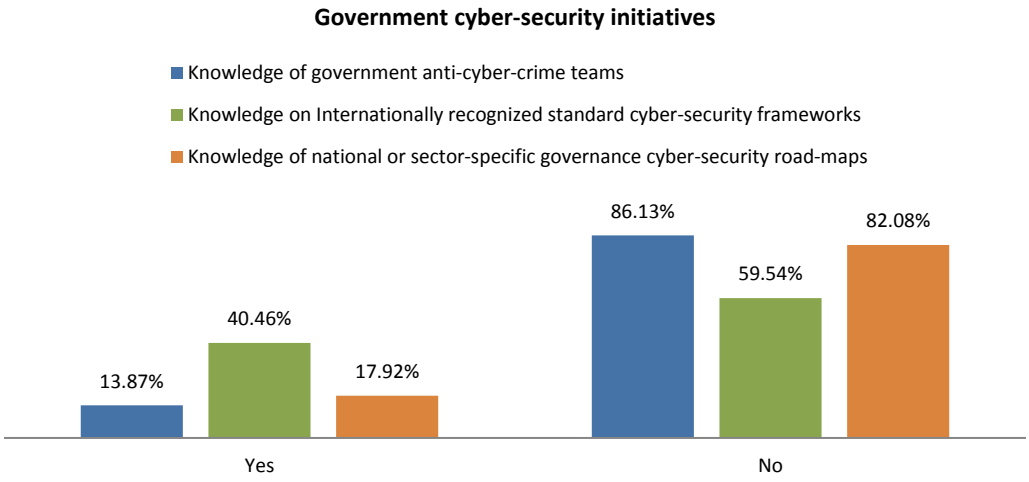


*Figure 4:13 Government cyber-security initiatives*

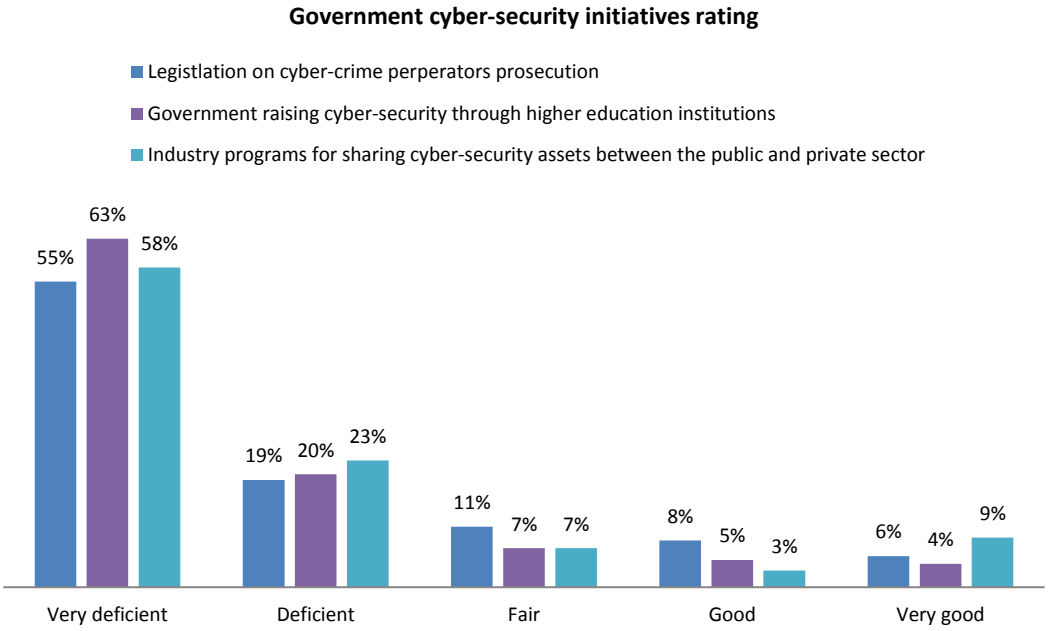


*Figure 4:14 Government cyber-security initiatives rating*

## 4.2 Diagnostic tests

### 4.2.1 Reliability Test

The initial pilot sample scored a co-efficient of 0.898, as we can see on table 4.2, that was greater than 0.7 adopted in this study, which justified the consistency of the questionnaire and hence the collection of data.

*Table 4:2 Reliability Statistics*

| Cronbach's Alpha | No of Items |
|---|---|
| .898 | 10 |

### 4.2.2 Factor Analysis

Factor analysis is a statistical procedure to identify interrelationships that exist among a large number of variables, i.e. identify how suites of variables are related (Cavana et al., 2001). Factor analysis can be used for exploratory or confirmatory purposes. In this study factor analysis was used for the former. Factor analysis for confirmatory purposes presupposes formulated hypotheses about the underlying structure of the variables and the research has an expected output to compare. Kaiser- Meyer-Olkin (KMO) measure and Bartletts tests were used to determine whether data collected was suitable for factor analysis and equally indicate whether sampling was adequate. KMO returns values between 0 to 1 and as a rule of thumb for interpreting statistics, a minimum KMO value acceptable is 0.5 (Cerny & Kaiser, 1977). Bartlett's test on the other hand checks for the strength of relationships between variables and should be less than 0.05 (Snedecor & Cochran, 1989). This study had factor analysis evaluating the strongest strategic leadership, government and cyber-security engineers' factors influencing or inhibiting cyber-security adoption by SMEs.

#### *4.2.2.1 Strategic Leadership factors affecting secure cyber-space*

KMO and Bartletts tests were run on four factors identified as influencing cyber-security adoption. KMO gave a high score of 0.787 while Barletts yielded a significance level of less than 0.05, indicating satisfactory sample and relationship strengths between variables as we can see from table 4.3.

Cerny & Kaiser (1977) states a correlation matrix gives the correlation coefficients between a single variable and every other variable in the investigation and any pair of variables with a value less than 0.5 can be dropped, which was done in this study.

*Table 4:3 KMO and Bartlett's Test*

| | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .787 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 462.994 |
| | df | 6 |
| | Sig. | .000 |

| Correlation Matrix | | Flexible Cost Structure (Pay as you use) | Quality support by product engineers | Ease of deployment | User friendly |
|---|---|---|---|---|---|
| Component | 1. Flexible Cost Structure (Pay as you use) | 1.000 | .589 | .541 | .537 |
| | 2. Quality support system by product engineers | .589 | 1.000 | .665 | .574 |
| | 3. Ease of deployment (e.g. quick to install) | .541 | .665 | 1.000 | .730 |
| | 4. User friendly (e.g. doesn’t require intensive training) | .537 | .574 | .730 | 1.000 |
| Sig. (1-tailed) | 1. Flexible Cost Structure (Pay as you use) | | .000 | .000 | .000 |
| | 2. Quality support system by product engineers | .000 | | .000 | .000 |
| | 3. Ease of deployment (e.g. quick to install) | .000 | .000 | | .000 |
| | 4. User friendly (e.g. doesn’t require intensive training) | .000 | .000 | .000 | |

The method of extraction used was standard Principal Component Analysis (PCA). PCA aims identifies underlying structures in data by extracting maximum variances, placing them into first factors, then removes variances explained by first factors to extract maximum variance for second factors (Cerny & Kaiser, 1977). The Eigenvalue table was divided into three sub-sections, i.e. component, Initial Eigen Values and Extracted Sums of Squared Loadings. For analysis and interpretation purpose this study was only concerned with Extracted Sums of Squared Loadings based on Eigen values greater than 1. From table 4.4 below we can see flexible cost structure component accounts for 70.5% of the variance with a 2.822 Eigen value.

*Table 4:4 Principal Component Analysis.*

| Component | Initial Eigen values | | | Extraction Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1. Flexible Cost Structure | 2.822 | 70.553 | 70.553 | 2.822 | 70.553 | 70.553 |
| 2. Quality support by product engineers | .526 | 13.151 | 83.704 | | | |
| 3. Ease of deployment | .404 | 10.107 | 93.811 | | | |
| 4. User friendly | .248 | 6.189 | 100.000 | | | |

An analysis was equally done to establish the impact level if any on leadership digital culture for SMEs that adopted cyber-security technology as we can see on results in table 4.5. It

was significant to note component one i.e. significant cost savings, was the only factor that had a high Eigen value greater than 1 at 3.292 with 65% variance.

*Table 4:5 Cyber-security adoption factors*

| Component | Initial | Extraction |
|---|---|---|
| 1. Significant Cost Savings due to reduced attacks and information loss | 1.000 | .574 |
| 2. Improved Operational Efficiency (i.e. reduced interruptions due to infected systems) | 1.000 | .696 |
| 3. Increased Customer retention (Lesser down times compared to competitors hence client retention and loyalty) | 1.000 | .673 |
| 4. Improved service quality (e.g. due to increased confidentiality and securing of client data) | 1.000 | .714 |
| 5. Business Growth | 1.000 | .635 |

| | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 3.292 | 65.844 | 65.844 | 3.292 | 65.844 | 65.844 |
| 2 | .609 | 12.183 | 78.027 | | | |
| 3 | .477 | 9.543 | 87.570 | | | |
| 4 | .345 | 6.897 | 94.467 | | | |
| 5 | .277 | 5.533 | 100.000 | | | |

#### 4.2.2.2 Strategic Leadership factors inhibiting secure cyber-space

As we can see from table 4.6, KMO and Bartletts tests were run on the 14 factors identified as inhibiting cyber-security adoption for enhanced secure cyber-space. KMO gave a high score of 0.849 while Barletts test of sphericity yielded a significance level of less than 0.05, indicating both sample and strength of the relationship between variables was satisfactory to proceed with meaningful factor analysis.

The principal component analysis yielded two components with Eigen values greater than one as illustrated in table 4.6 above. The two components, lack of finances and lack of management support account for 70.128% of total variance with each having an Eigen value/rotation sum of squared loadings 5.8 and 4.018 respectively. According to Cerny & Kaiser (1977), a rotation method makes it more reliable to understand and interpret output. Eigen values do not affect the rotation method, but the rotation method affects the Eigenvalues or percentage of extracted variances. The study opted for varimax rotation with Kaiser normalization (Cerny & Kaiser, 1977). The rotation method showed strong component loadings or correlations between the two factors as we can see in table 4.7.

Varimax rotated component analysis was critical in reducing the fourteen initially identified factors to two significant main components. The highest individual loadings for each factor were categorized under each component to further explain the variance.

*Table 4:6 Strategic Leadership factors inhibiting secure cyber-space*

| Components inhibiting cyber-security adoption for enhanced secure cyber-space. | Initial Values assigned by SPSS before running tests. |
|---|---|
| 1. Lack of Finances | 1.000 |
| 2. Lack of Management Support | 1.000 |
| 3. Lack of awareness on cyber-security cloud technologies | 1.000 |
| 4. Lack of skills or required competence | 1.000 |
| 5. Complexity of migration | 1.000 |
| 6. Incompatibility with existing systems | 1.000 |
| 7. No perceived tangible benefits | 1.000 |
| 8. Privacy Concerns | 1.000 |
| 9. Security | 1.000 |
| 10. Loss of Control to third parties | 1.000 |
| 11. Difficulty in Migration | 1.000 |
| 12. Vendor Lock-in | 1.000 |
| 13. Ability to scale | 1.000 |
| 14. Service Availability & Reliability | 1.000 |

| Components | Initial Eigenvalues after running tests | | | Rotation Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 8.352 | 59.657 | 59.657 | 5.800 | 41.429 | 41.429 |
| 2 | 1.466 | 10.471 | 70.128 | 4.018 | 28.699 | 70.128 |
| 3 | .900 | 6.430 | 76.558 | | | |
| 4 | .727 | 5.196 | 81.754 | | | |
| 5 | .526 | 3.759 | 85.513 | | | |
| 6 | .518 | 3.702 | 89.215 | | | |
| 7 | .401 | 2.861 | 92.076 | | | |
| 8 | .306 | 2.182 | 94.258 | | | |
| 9 | .224 | 1.598 | 95.856 | | | |
| 10 | .194 | 1.389 | 97.245 | | | |
| 11 | .134 | .958 | 98.203 | | | |
| 12 | .110 | .784 | 98.987 | | | |
| 13 | .093 | .663 | 99.651 | | | |
| 14 | .049 | .349 | 100.000 | | | |

*Table 4:7 PCA - Varimax with Kaiser Normalization*

| **Rotated Component Matrix** | **Component** | |
|---|---|---|
| | **1** | **2** |
| Complexity of migration | .887 | |
| Lack of skills or required competence | .870 | |
| Vendor Lock-in | .846 | |
| Incompatibility with existing systems | .811 | .329 |
| Lack of awareness on cyber-security cloud technologies | .736 | .312 |
| Difficulty in Migration | .699 | .318 |
| No perceived tangible benefits | .654 | .408 |
| Lack of Management Support | .626 | .444 |
| Ability to scale | .588 | .549 |
| Privacy Concerns | | .897 |
| Security | | .854 |
| Loss of Control to third parties | | .773 |
| Lack of Finances | .464 | .678 |
| Service Availability & Reliability | .561 | .562 |

| **Component** | **Factors** | **Co-efficient** | |
|---|---|---|---|
| ***Lack of finances*** | Complexity of migration | .887 | Component 1 |
| | Lack of skills or required competence | .870 | |
| | Vendor Lock-in | .846 | |
| | Incompatibility with existing systems | .811 | |
| ***Lack of management support*** | Privacy Concerns | .897 | Component 2 |
| | Security | .854 | |
| | Loss of Control to third parties | .773 | |

Under Component 1*(Lack of finances*), respondents view lack of finances from varying points in a descending order based on analyzed co-efficient. the SME leaders main concerns can be clustered as lack of finances to facilitate a rather complex migration to a secure cyber space (0.887), they lack finances to facilitate acquisition of requisite competence once the organization moves to secure cyber technologies (0.870), they view vendor lock in and associated annual support costs as having prohibitive costs that they cannot afford (0.846) and lack of finances to ensure that their current systems are compatible with cyber security technologies (0.811).

On the other hand, under component 2 *(lack of management support)* respondents view lack of management support from varying points. Likewise in a descending order based on analyzed co-efficient, the SME leaders main concerns can be clustered as lack of management support for requisite privacy (0.897), lack of management support for providing requisite network security (0.854), lack of management support due to non-desired effect of losing direct control of company IT systems to a third party who guarantees cyber security (0.773) and lack of management support as a result of the related cost/financial outlay as a result of purchasing cyber security technologies (0.678).

#### 4.2.2.3 Government factors affecting secure cyber-space

The factors were codified as follows for purposes of input into SPSS for analysis.

- V97 – Criminal legislation regarding cyber-security in Kenya.
- V99 – Cyber-security higher education and professional training programs in Kenya noting that higher education in Kenya is regulated by the government.
- V101- Government-private sector programs for sharing cyber-security resources like cyber-intrusion deterrent teams.

A correlation matrix was equally provided showing the variables relationships by providing correlation coefficients between single variable and every other variable in the investigation as we can see in table 4.8.

*Table 4:8 Coded Government factors*

| | | Initial | Extraction | |
|---|---|---|---|---|
| V97 | | 1.000 | | .695 |
| V99 | | 1.000 | | .728 |
| V101 | | 1.000 | | .812 |
| | | V97 | V99 | V101 |
| Correlation | V97 | 1.000 | .531 | .640 |
| | V99 | .531 | 1.000 | .679 |
| | V101 | .640 | .679 | 1.000 |
| Sig. (1-tailed) | V97 | | .000 | .000 |
| | V99 | .000 | | .000 |
| | V101 | .000 | .000 | |

KMO measure yielded a score of 0.696 while Barletts test of sphericity had a significance level of less than 0.05. The principal component analysis yielded only one component solution therefore a varimax rotation could not be performed. From table 4.9 we can see V97 (Criminal legislation regarding cyber-security in Kenya) accounted for 74.486% of the variance with a 2.235 Eigen value. Thus, most respondents view the criminal legislation regarding cyber-security in Kenya, a significant factor that would influence their cyber-security adopting rate. V99 and V101 contributed 15.736% and 9.778% of total variance explained respectively therefore regarded as statistically insignificant.

*Table 4:9 Government factors affecting secure cyber-space*

| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| V97 | 2.235 | 74.486 | 74.486 | 2.235 | 74.486 | 74.486 |
| V99 | .472 | 15.736 | 90.222 | | | |
| V101 | .293 | 9.778 | 100.000 | | | |

.

# Chapter 5: Discussions, Conclusion and Recommendation

## 5.1 Introduction

The study was guided by the general objectives; To assess strategic leadership, government and cyber-security product engineers' factors affecting cyber-security adoption by SMEs in Kenya.

## 5.2 Summary

**Cyber-security budget**

Having found 43% of respondents with an annual turnover of Kshs 500,000 and 5 million, the study collated this with literature that identified small or insignificant cyber-security budgets for SMEs. Serianu (2015) states 90% of organizations in Kenya are allocating less than Kshs 500,000 annually for cyber-security measures. This can be interpreted to mean at least 10% of the annual turnover showing small budget might not be negligence but careful considerations of costs versus annual turnover. With this established fact, the study recommends future study that deeply delineate how SME cyber-security budget is used to understand if crucial components are covered because with increased cyber-space, SME annual turnover will increase as cyber-attack costs reduce.

**Leadership is not aware of the importance of sound cyber-strategies**

The study found while most SME neglect important areas like business continuity, disaster recovery and legal compliance which are critical issues in the current cyber-era as we can see in figure 4.5. This shows most SMEs take advantage of technology to automate some functions but are may be not aware of increased cyber-threats and cyber-strategies that would best prepare for threats eventualities. The study thus corroborates the findings of Migiro (2006) that identifies the dearth of computer skills as a key problem in correct use of technology, making leaders not sure which cyber-security strategies to adopt as we can see in table 4.1. This study thus recommends

increased creation of cyber-strategies awareness through government programs as well us private institutions participation since cyber-security is a collective effort and also more higher education training on cyber-security skills.

**Leadership knowledge on Cyber-Security Strategies Vs Preparedness for Cyber-threats**

The study found it abstruse that most respondents were confident of how well they were prepared for cyber-attacks, yet not so confident of their cyber-strategies as can be seen in figure 4.6. Since most of the respondents had general management duties in their job functions, the study collates that most respondents had leadership duties in their respective business roles. This then leads the study to conclude the perceived preparation against cyber-attacks by SME leaders is misguided and plays a role in secure cyber-space provision. If the leaders are not confident of their cyber-strategies then they should not consider their businesses are well prepared for cyber-attacks unless they are operating with a false sense of security. Barton et al. (2016) could not find a correlation between normative influences and senior management belief, normative influences and senior management participation, coercive influences and senior management participation. This can be explained with the false sense of security leaders exhibited in this study.

**Reason for not adopting cyber-security to provide enhanced secure cyber-space**

The study found that as much as lack of finances was largely attributed to lack of adopting cyber-security measures, lack of management support influenced by lack of finances was the main reason for lack of cyber-security adoption. The study found great considerations (70%) by SME leaders put a lot of weight on affordability/cost as a factor influencing management support for adopting cyber-security. This also corroborates findings of this study that most (50%) qualified skills existing in SMEs are relevant diploma in cyber-security, which is relevantly financially cheaper to achieve than advanced professional certificates (6.9%) or master's degree (9.2%) in

cyber-security. Apart from cost, lack of management support is also supported with SME leaders major concern on complexity in migration with a 0.89 co-efficient and lack of required skills with a 0.87 co-efficient. Kimwele et al. (2005) also tried to address this challenge by providing a cost-effective framework but this study recommends a research gap to be filled by improving Kimwele et al. (2005) framework, to connect cost influence on management support and not cyber-security products.

**Government role in secure cyber-space**

The major factor (74%) that would influence SMEs participation in enhancing secure cyber-space is if cyber-laws were enacted that would ensure cyber-criminals are persecuted effectively. Without such cyber-laws, most leaders (74%) do not see a reason to engage in effective cyber-security measures. Government should enact cyber-laws that will make investment into cyber-security worthwhile for SMEs. Government should also ensure cyber-security education levels are increased in institutions of higher education to help leaders understand cyber-security strategies better. The government should also increase aware on national roadmaps in place geared towards protection of business resources since SMEs are eager to engage and exchange cyber-security assets. Mandelcorn et al. (2013) attribute increased cyber-threat to the absence of a capable defender leaving SMEs vulnerable to motivated offenders. The absence of a defender is thus seen in the findings of this study that cyber-laws in Kenya are completely wanting and urgently required as seen in figure 4.1. As an independent variable, if cyber-laws existed then SMEs would have an enhanced secure cyber-space to change findings of Migiro (2016) who states government efforts so far are not working.

While cyber-security is a well-researched and highly regarded topic in today's market, there is a lot of ambiguity blurring leadership strategies trying to protect business resources. Cyber-

security can only be improved as a collective effort between SME leaders and government. Cyber-threats have increased tremendously and the Kenyan economy stands to be negatively impacted by cyber-threats which mainly target SMEs. Leaders are mainly concerned with flexible cost (pay as you used instead of one-time purchase) and availability of skills.

In future the study will focus on assessing cyber-security adoption in a developed country, to understand if same independent variables differ in impact to cyber-security adoption and cyber-space.

# References


Abimbola, T., & Vallaster, C. (2007). Brand, organizational identity and reputation in SMEs: an overview. *Qualitative Market Research: An International Journal, 10*(4), 341 - 348.

Ahlgreen, M. (2010, December). When the Business of Business Became Everybody's Business. Retrieved January 16, 2018 from http://ibde.org/component/content/article/114-when-the-business-of-business-became-everybodys-business.html

Amaratunga, D., Baldry, D., Sarshar, M., & Newton, R. (2002). Quantitative and qualitative research in the built environment: application of "mixed" research approach. *Work Study, 51*(1), 17–31. Retrieved January 16, 2018 from https://doi.org/10.1108/00438020210415488

Bailey, T., Kaplan, J., & Rezek, C. (2014, June). Why senior leaders are the front line against cyberattacks | McKinsey & Company. Retrieved January 23, 2018, from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

Barkan, S. (2006). *Criminology: A sociological understanding (3rd ed.).* Upper Saddle River, NJ: Prentice Hall.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security, 59*, 9–25. Retrieved January 23, 2018 from https://doi.org/10.1016/j.cose.2016.02.007

Bateman, I. J., Carson, R. T., Day, B., Hanemann, M. W., Hanley, N., Hett, T., Swanson, J. (2002). *Economic Valuation with Stated Preference Techniques: A Manual*. Cheltenham, UK: Edward Elgar.

Beck, T., Demirguc-Kunt, A., & Levine, R. (2005). SMEs, growth, and poverty: cross-country evidence. *Journal of economic growth*, *10*(3), 199-229.

Belias, D., & Koustelios, A. (2014). The impact of leadership and change management strategy on organizational culture. *European Scientific Journal, ESJ*, *10*(7).

Blanche, T., Durrheim, M., & Painter, K. (2006). *Research in practice: Applied methods for the social sciences* (2nd Edition). Cape Town: UCT Press.

Cartelli, A. (2007). Socio-Technical Theory and Knowledge Construction: Towards New Pedagogical Paradigms? *Issues in Informing Science and Information Technology*, *4*, 001-014. Retrieved January 10, 2018 from https://doi.org/10.28945/928.

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing. *Journal Computers in Human Behavior*, *29*(6), 2156–2160. Retrieved January 10, 2018 from https://doi.org/10.1016/j.chb.2013.05.009

Cavana, R. Y., Delahaye, B. L., & Sekaran, U. (2001). *Applied Business research: Qualitative and Quantitative Methods*. Australia, Milton, Queensland: John Wiley & Sons.

Central Bank of Kenya. (2017). Guidance Note On Cyber-Security For The Banking Sector. CBK. Retrieved from January 12, 2018 from https://www.centralbank.go.ke/wp-content/uploads/2017/09/GUIDANCE-NOTE-ON-CYBERSECURITY-FOR-THE-BANKING-SECTOR.pdf

Chak, S. K. (2015). *Managing Cybersecurity as a Business Risk for Small and Medium Enterprises* (PhD Thesis).

Cerny, C.A., & Kaiser, H.F. (1977). A study of a measure of sampling adequacy for factor-analytic correlation matrices. Multivariate Behavioral Research, 12(1), 43-47.

Cisco. (2017). *Annual Cybersecurity Report.* San Jose, CA: Cisco Systems, Inc.

Das, S., Nayak, T., Dept, A.-P., & University, C. (2013). IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. *International Journal of Engineering Sciences*, *6*(2), 142–153.

Denscombe, M. (2014). The good research guide: for small-scale social research projects. McGraw-Hill Education (UK).

Dunn Cavelty Myriam. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. Retrieved on January 12, 2018 from https://doi.org/10.1007/s11948-014-9551-y

Evans, D. (2011). *The Internet of Things How the Next Evolution of the Internet Is Changing Everything.* Retrieved on January 12, 2018 from Cisco Internet Business Solutions Group: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Gary Miller. (2016). GEM Strategy Management. Retrieved January 16, 2018, from https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business

Goodman, H., & Traynor, P. (2013). Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology and Arts 8*, 2435-64.

Grayson, D. (2011). Embedding corporate responsibility and sustainability: Marks & Spencer. *Journal of Management Development*, *30*(10), 1017–1026.

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

Henry, G. T. (1990). *Practical Sampling* (Vol. 21 of Applied Social Research Methods). SAGE, 1990.

Higon, D. A. (2011). The impact of ICT on innovation activities: evidence for UK SMEs. *International Small Business*, 684–699.

ICTA. (2014). *National Security Strategy.* Retrieved on January 12, 2018 from ict.go.ke: http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf

International Telecommunication Union. (2017). *Global Cybersecurity Index 2017*. Geneva, Switzerland: International Telecommunication Union (ITU).

Kathuri, J. N. & Pals, D. A. (1993). Introduction to Educational Research. Njoro. Egerton University Press

Kenya National Bureau of Statistics. (2016). *MSME Basic Report*. Nairobi: Kenya National Bureau of Statistics. Retrieved on January 12, 2018 from https://www.knbs.or.ke/download/2016-msme-basic-report

Kimwele, M., Mwangi, W., & Kimani, S. (2005). *Success through information security knowledge: proceedings of the IFIP TC11 WG 11.8 Four World Conference Information Security Education, (WISE4), 18-20 May 2005, Moscow, Russia*. Moscow: Moscow Engineering Physics Institute (State University).

KPMG. (2016). *Small Business Reputation & the Cyber Risk.* Retrieved January 12, 2018 from KPMG: http://www.kpmg.com/channelislands/en/about/Documents/small-business-reputation-and-the-cyber-risk.pdf

Kurpius, S., Stafford, M. (2006). *Testing and measurement: A user friendly guide*. Los Angeles, CA: Sage.

McClimans, F., Fersht, P., Snowdon, J., Phelps, B., & LaSalle, R. (2016). The State of Cybersecurity and Digital Trust 2016. Retrieved on January 12, 2018 from https://www.accenture.com/t20160704T014005Z__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf

Mandelcorn, S., Modarres, M., & Mosleh, A. (2013). *An Explanatory Model of Motivation for Cyber-Attacks Drawn from Criminological Theories*.

Matambalya, F., & Wolf, S. (2001). *The role of ICT for the performance of SMEs in East Africa: empirical evidence from Kenya and Tanzania*. ZEF Discussion Papers on Development Policy.

Michiels, S., & Crowder, V. (2001). Discovering the 'Magic Box': Local Appropriation of Information and Communication Technologies (ICTs). Rome, Italy.

Migiro, S. O. (2006). Diffusion of ICTs and E-commerce adoption in manufacturing SMEs in Kenya. *South African Journal of Libraries and Information Science*, *72*(1), 35–44.

Morgan, S. (2016, August 12). Cybercrime Damage Costs $6 Trillion in 2021, Cybersecurity Market Data. Retrieved January 10, 2018 from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

Morgan, S. (2017a). 2017-Cybercrime-Report. Cybersecurity Ventures. Retrieved March 12, 2018 from CybersecurityVentures.com

Morgan, S. (2017b). Protect Your Small Business From Cyber Attacks With These Free Tools. Retrieved March 12, 2018 from https://www.entrepreneur.com/article/301193

Mutegi, C. (2015, November). Jua Kali sector plays key role in economic development and job creation. Retrieved January 16, 2018, from http://www.mygov.go.ke/smes-play-key-role-in-economic-development-and-job-creation

Nicol C. (2003) ICT Policy: A Beginner's Handbook. The Association for Progressive Communications.

NSBA. (2014). *2014 Year-end Economic Report.* Retrieved March 15, 2018 from http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf

NSBA. (2015). *2015 Year-end Economic Report.* Retrieved January 21, 2018 from http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116.

Redmiles, E. M., Acar, Y., Fahl, S., & Mazurek, M. L. (2017). A Summary of Survey Methodology Best Practices for Security and Privacy Researchers, 10.

Robert Jervis. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2). Retrieved January 12, 2018 from http://www.sscnet.ucla.edu/polisci/faculty/trachtenberg/guide/jervissecdil.pdf

Roscoe, J. T. (1975). *Fundamental research statistics for the behavioral sciences* (2nd Edition). New York: Holt Rinehart & Winston.

Rowe, F. (2014). What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255. Retrieved March 18, 2018 from https://doi.org/10.1057/ejis.2014.7

Serianu. (2015). *Kenya Cyber Security Report 2015*. Nairobi, Kenya: Serianu Cyber Threat Intelligence Team. Retrieved March 18, 2018 from http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf

Serianu. (2016). *Kenya Cyber Security Report 2016*. Nairobi, Kenya: Serianu Cyber Threat Intelligence Team. Retrieved March 18, 2018 from http://serianu.com/downloads/KenyaCyberSecurityReport2016.pdf

Shamoo, A. E., & Resnik, D. B. (2003). *Responsible Conduct of Research* (Third Edition). Oxford University Press.

Snedecor, George W. and Cochran, William G. (1989), Statistical Methods, Eighth Edition, Iowa State University Press.

Spidalieri, F. (2016). Understanding Cyber Threats - Lessons For The Boardroom. Presented at the Understanding Cyber Threats in the Boardroom, Newport, Rhode Island: Salve Regina University's Pell Center.

Symantec. (2016). *2016 Internet Security Threat Report*. Symantec.

Verizon. (2017). *Verizon's 2017 Data Breach Investigations Report*. Retrieved March 18, 2018 from https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Zikmund, W. G. (1997). *Business Research Methods* (5, illustrated, reprint ed.). Dryden. Retrieved March 18, 2018 from http://www.industrialization.go.ke/index.php/policies/99-micro-and-small-enterprises-act-2012

# Appendices:

## Appendix 1: Questionnaire

**A Study on Exploring Strategic Leadership in Cyber-Security in Kenya: A Case of SMEs**

Participation is voluntary and all data will be treated as anonymous and confidential. The questions concern various aspects of business or department. Answer by circling/ticking/cross the option/number which best corresponds to your opinion. There is no right or wrong answers. Read the questions carefully and consider your chosen number as it will correspond to your opinion.

We appreciate your contribution and thank you for your time.

Contacts: sbsericm@gmail.com

Phone: 0721577097

Affiliation: Strathmore Business School

# Cyber-Security Questionnaire

**First Name:** **Last Name:**

**Company Name:**

**Date:** **Contact:**

**QUESTIONNAIRE**

**Instructions:** Please indicate your answer with a **tick (√)** on the checkbox when presented with options.

**SECTION A: BACKGROUND INFORMATION**

1. Do you have less than 100 employees in your business?

2. In what industry sector does your business currently operate?
   - ☐ Wholesale/Retail trade/Repair of Motor Vehicles/Motorcycles
   - ☐ Accommodation and Food Services
   - ☐ Manufacturing
   - ☐ Other Service Activities Specify_____

3. What is the approximate **annual** turnover of the business in Kshs?
   - ☐ Less than 500,000
   - ☐ Between 500,000 and 5 Million
   - ☐ Between 5 Million and 100 Million
   - ☐ More than 100 Million

4. How long has your business been in existence?
   ☐ Less than 5 years ☐ 5 – 10 years ☐ 10 – 20 years ☐ More than 20 years

5. How would you describe your primary job function?
   - ☐ General Management
   - ☐ Administration & Operations
   - ☐ Human Resources
   - ☐ Other Specify _____
   - ☐ Sales & Marketing
   - ☐ Finance & Accounting
   - ☐ IT

**SECTION B: STRATEGIC LEADERSHIP FACTORS INFLUENCING CYBER-SECURITY ADOMAIN**

**Tick where appropriate for the questions below. Use the scale below for ratings:**
**1 Very 2 Low 3 Moderate 4 High 5 Very High**

6. What is your job level?
   - ☐ Manager Level
   - ☐ Owner of business
   - ☐ Director Level
   - ☐ Supervisor Level
   - ☐ Operational

7. On a scale of 1 to 5, with 5 being 'Very High', how would you rate your knowledge or understanding of Cyber-security technologies and strategies?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

8. On a scale of 1 to 5, with 5 being 'Very High', how would you rate the frequency of updating organization wide software installed to detect threats?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

9. On a scale of 1 to 5, with 5 being 'Very High', how would you rate the frequency of notifications given to staff on cyber-intrusion attempts? (i.e. Are company's 'information' assets custodian staff cautious on all alerts?)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

10. On a scale of 1 to 5, with 5 being 'Very High', how would you rate the follow up made when threats have been detected and eliminated? (i.e. Is there an analysis of a blocked intrusion attempt or reverse engineering of malware e.g. to determine the type of threat)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

11. Who handles your IT Cyber-security operations?

☐ In-house staff or Employees Partly Outsourced

☐ Completely Outsourced

12. Have you deployed cyber-security measures in your business? (e.g. use of anti-virus on computers)

☐ YES ☐ NO

**If YES, continue with this section. If NO, please proceed to question 20.**

13. What is your level of preparedness in case of a cyber-attack? (Is your security software / mechanisms effective/Is it updated e.g. in detecting threats i.e. virus)

☐ Very Low ☐ Low ☐ Moderate ☐ High ☐ Very High

14. In which business functions have cyber-security Strategies been deployed? (Check all that apply)

☐ Email & Communication

☐ Sales & Marketing

☐ Inventory & Supplies Management

☐ Data Backup & Storage

☐ Finance & Accounting

☐ Customer Relationship Management (CRM)

☐ HR & Payroll

☐ Enterprise Resource Planning (ERP)

Other, Specify _____

a. On a scale of 1 to 5 (1 being 'Very Low' and 5 'Very High') rate how the following factors influenced your decision to adopt your chosen cyber-security technology

| **Factor** | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Flexible Cost Structure (Pay as you use) | | | | | |
| Quality support system by product engineers | | | | | |
| Ease of deployment (e.g. quick to install) | | | | | |
| Ability to scale | | | | | |
| User friendly (e.g. doesn't require intensive training to operate) | | | | | |

b. Has the use of cyber-security technology had any significant impact on your business?

☐ YES ☐ NO

c. If yes to the above, how would you rate the **level of impact** of the following factors: (1 being 'Very Low' and 5 'Very High')

| **Factor** | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Significant Cost Savings due to reduced attacks and information loss | | | | | |
| Improved Operational Efficiency (i.e. you have experienced reduced interruptions at work due to infected systems) | | | | | |
| Increased Customer retention (Are you having lesser down times compared to competitors hence client retention and loyalty) | | | | | |
| Improved service quality ( e.g. due to increased confidentiality and securing of client data) | | | | | |
| Business Growth | | | | | |

d. Cyber-security skills are in your business?

| **Skill** | How many? |
|---|---|
| Professional Certificate in Cyber-Security | |
| Relevant Bachelor's Degree in Cyber-Security | |
| Relevant Master's Degree in Cyber-Security | |
| Relevant Diploma in Cyber-Security | |
| Relevant Outsourced Contracts | |

15. Information Technology (IT) is a crucial part of your organizational strategy:

☐ Strongly Agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly Disagree

16. Do you have a Cyber-Security Strategic Plan that is part of your overall organizational strategic plan?

YES ☐ NO ☐

***If YES, what are the core issues covered?***

☐ Business Process Automation
☐ Information Management
☐ Business Continuity & Disaster Recovery
☐ On-Premise / Off-Premise hosting of applications
☐ Legal and compliance
☐ Resource Management
☐ Others…….. Specify ……..

17. Do you have a dedicated IT Cyber-security budget?

YES ☐ NO ☐

If yes, what is the estimated annual allocation in Kshs?

☐ Less than 500, 000
☐ Between 500,000 and 1 Million
☐ Between 1 Million and 3 Million
☐ Over 3 Million

18. How many years of experience do you have with information technology products?

☐ Less than 5yrs ☐ 5-10 yrs ☐ 11-15yrs ☐ 16-20yrs ☐ Over 20yrs

19. Do you have professional qualifications specific to Cyber-security or Cyber-crime prevention/deterrent?

YES ☐ NO ☐

If yes please specify which one you hold:

**Answer these questions if you said NO on question 12**

20. How would you rate the following to be the reasons for not going for Cyber-Security Technology?

a) Use the key below:

1 Strongly Disagree 2 Disagree 3 Neutral 4 Agree 5 Strongly Agree

| **Factor** | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Lack of Finances | | | | | |
| Lack of Management Support | | | | | |
| Lack of Awareness on Improved Cyber-Products | | | | | |
| Lack of skills or required competence | | | | | |
| Complexity of migration | | | | | |
| Incompatibility with existing systems | | | | | |
| No perceived tangible benefits | | | | | |
| Privacy Concerns | | | | | |
| Security | | | | | |
| Loss of Control to third parties | | | | | |
| Difficulty in Migration | | | | | |
| Vendor Lock-in | | | | | |
| Ability to scale | | | | | |
| Service Availability & Reliability | | | | | |

b) To what extent would the following influence or change your decision on adoption of Cyber-security technologies?

| **Factor** | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Competitive pressure | | | | | |
| Changes in the market or industry you operate in | | | | | |
| Proper laws and regulations | | | | | |
| Support and training from cyber-security service providers | | | | | |

**SECTION C: ASSESSING GOVERNMENT POLICIES AFFECTING CYBER-SECURITY DOMAIN**

21. Are you aware of any specific regulation regarding cyber-security and compliance requirements?

YES ☐ NO ☐

If YES, how knowledgeable are your employees with cyber security related legislation requirements and its related penalties. *Use the scale below for ratings:*

*1 Very deficient 2 Deficient 3 Fair 4 Good 5 Very good*

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

If NO, how would you rate the urgency with which it is required for purposes of a robust SME business environment?

☐ Immediate urgency ☐ Very urgent ☐ Fairly urgent ☐ Not urgent ☐ Can wait

22. Are you aware of any officially approved national or sector-specific Cyber-security deterrent team(s)? (anti-cyber-crime teams)

YES ☐ NO ☐

*If YES, how would you rate their effectiveness as regards assisting in-house company IT teams in responding to cyber-attacks?*

*1 Very deficient 2 Deficient 3 Fair 4 Good 5 Very good*

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

23. Are you aware of any officially-approved national (and sector specific) cyber-security frameworks for implementing internationally recognized cyber-security standards?

YES ☐ NO ☐

If YES, how would you rate its inclusivity as relates consulting varied SME industry stakeholders and strategic leaders

*1 Very deficient 2 Deficient 3 Fair 4 Good 5 Very good*

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

24. Are you aware of any officially recognized national or sector-specific governance roadmap for cyber-security?

YES ☐ NO ☐

If YES, do you agree that it will lead to an improved business environment?

☐ Strongly Agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly Disagree

25. Would your organization be open to considering having a strategic cyber plan where joint SME stakeholders with the government agreed on annual **cyber audits**?

☐ Very likely ☐ Likely ☐ Neutral ☐ unlikely ☐ very unlikely

**Tick where appropriate for the questions below. Use the scale below for ratings:**
**1 Very deficient 2 Deficient 3 Fair 4 Good 5 Very good**

| QUESTIONS | Write comments here in case you would like to specify on any question | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 Kindly rate the current criminal legislation regarding cyber activities in Kenya? (Are you confident perpetrators can be prosecuted?) | | | | | | |
| 2. How would you rate the national or sector-specific educational and professional training programs in Kenya aimed at raising awareness with the general public to promote cyber-security among higher education institutions or professional bodies. | | | | | | |
| 3. How would you rate the current industry programs for sharing cyber-security assets between the public and private sector? (If any, please specify) | | | | | | |


**Thank you for taking time to answer this questionnaire**