THE UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS

Human Factors Affecting Favourable Cybersecurity Culture: A Case of Small and Medium-sized Enterprises (SMEs) Providing Enterprise wide Information Systems Solutions in Nairobi City County in Kenya

BY

GEORGE M. NJOROGE

P54/72805/2014

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

JULY 2020

DECLARATION

I declare that this is my original work and has not been presented for a degree in any other University.

Signature…….. **Date……**

George Mwathi Njoroge

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

Signature…….. **Date……**

Professor Agnes N. Wausi

ACKNOWLEDGEMENTS

First and foremost, I extol the most high God for helping me get this far. This research work wouldn't also have materialized had it not been the support, guidance and encouragement from a number of people. My sincere appreciation is to my project supervisor, Professor Agnes N. Wausi, for finding adequate time to review this work and offer very helpful feedback. I am also very indebted to the other panelists for the constructive critique and valuable contribution that helped in shaping this project. I am so thankful to Margaret, my dear wife and Marcus, my loved son for your patience and restraint in many occasions I had to sacrifice some family time towards this project. I am exceptionally grateful to all my relatives for their goodwill and prayers, especially my mum who at one time contributed for my school fees as an academic blessing. I convey appreciativeness to all the SMEs companies that voluntary participated in this research and in particular their willingness to provide information that made it possible for completion of this project. To the entire School of computing community, your support in one way or the other is appreciated, may God bless you all.

ABSTRACT

Recent news coverage in both print and electronic media clearly indicates that cyberattacks are increasingly on the rise. As compared to large enterprises, SMEs are highly vulnerable to cyberattacks for they lack adequate cybersecurity controls in place to cope up with evolving cyber threats. According to reports from the industry, humans are regarded as the root cause of many cybersecurity incidents in organizations.

This study, thus, purposed to examine the key human factors that impact on favourable cybersecurity culture in Kenyan SMEs premised in Nairobi City County and that provides enterprise wide Information Systems(IS) solutions. Primary data was collected through mail survey method from 34 SMEs that were selected from the official 2019 yellow pages Kenya online directory. The data collection tool was a structured questionnaire. To achieve this, quantitative research inform of descriptive research design was conducted. Judgmental sampling technique was used to choose respondents believed to have the required information relating to the objective of the study. As such, the respondents for the study consisted of senior personnel responsible for cybersecurity issues, the Information and Communication Technology (ICT) head, technical ICT staff and a general user of ICTs in each of the selected SME. Statistical Package for Social Sciences version 23(SPSS) was used for data analysis.

Descriptive analysis findings established perceptions regarding the current cybersecurity practices in the SMEs studied. The regression analysis results of all the independents variable against the dependent variable jointly accounted for 54.4% (R-square equals to 0.544) of variation in the dependent variable (favourable cybersecurity culture). 45.6% of variation in favourable cybersecurity culture was therefore unexplained for, and this are covered by other factors not considered in the study. The P-value of 0.000(<0.05) implied that the model used to predict the effect of key human factors on favourable cybersecurity culture among SMEs providing enterprise wide IS solutions was statistically significant at the 5% significance level. Further, it was established that top management support and involvement together with reward and deterrence measures are positive and significant predictors of favourable cybersecurity culture among SMEs providing enterprise wide IS solutions and thus form important strategies for instilling favourable cybersecurity culture in SMEs providing enterprise wide IS solutions in Nairobi city county. Other strategies that need to be developed by these SMEs are cybersecurity policy, cybersecurity change management, cybersecurity training and awareness programs, cybersecurity monitoring and audit for they were also found to have a positive effect on favourable cybersecurity culture.

The study concludes by emphasizing the need for adequate and consistent top management support and involvement in cybersecurity issues. It recommends that the top management need to strongly recognise their critical role in ensuring favourable culture of cybersecurity in organizations. Similar to road maps that clearly show direction and distance, the roadmap developed from this study can be used by cybersecurity practitioners to benchmark cybersecurity practices and processes in efforts to promote favourable cybersecurity culture in their organizations

Keywords: Cyberattacks, enterprise wide IS solutions, human Factors, organizational security culture, cybersecurity roadmap, Small and Medium Enterprises(SMEs)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

BYOD	Bring Your Own Device
CAK	Communication Authority of Kenya
CBK	Central Bank of Kenya
DoS	Denial of Service
ENISA	European Network and Information Security Agency
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ICTs	Information and Communication Technologies
IoT	Internet of Things
IS	Information Systems
IT	Information Technology
KRA	Kenya Revenue Authority
ISO	International Organization for Standardization
ISACA	Information Systems Audit and Control Association
ISMS	Information security management system
PSP	Payment service providers
PWC	PricewaterhouseCoopers
SCT	Social Cognitive Theory
SPSS	Statistical Package for Social Sciences version 23
SME	Small and medium-sized businesses
TB	Terabyte

CHAPTER ONE

1.0 INTRODUCTION

The subheadings covered in this chapter include: Background of the study, Problem statement, Research objectives, Significance of the study, Limitations and Basic assumptions of the study and Definition of terms. The subheading on significance of the study describes the motivation that led to the study among SMEs that provide enterprise wide IS solutions.

1.1 Background of the Study

Cybersecurity culture in organization relates to people behavior when interacting with Information and Communication Technologies (ICTs). It "refers to the knowledge, attitude, assumptions, norms, perceptions, values, and beliefs of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies" (ENISA, 2017, p. 5). Within an organizational context, familiar topics surrounding cybersecurity culture and that are associated with cybersecurity as discussed by Gartner (2013) include offensive security, information security, operational technology security and Information Technology(IT) security. The management of all these topics in organizations, often referred to as cybersecurity management, is usually handled through cybersecurity management programs. Organizational cybersecurity management program is therefore a systematic approach designed to manage cybersecurity initiatives in organization and is comprised of technology, process and people aspects of cybersecurity (ENISA, 2017) that are aimed to safeguard the availability, confidentiality and integrity of organizational strategic assets. Regarding the technology, process and people aspects, cybersecurity culture concerns itself with the people side of cybersecurity management.

The rapid growth of ICTs has significantly transformed the way organizations deal with their respective customers, employees and third parties (Rasha & Othman, 2016). Many organizations have therefore adopted IS to enhance operational efficiency and competitive advantage. Although the adoption of IS has brought about lot of benefits to organizations and their stakeholders, valuable organizational assets have largely been exposed to cyber-attacks. Denial of Service (DoS), malwares, web application attacks and system vulnerabilities (CAK, 2019), social engineering, phishing and ransomware (Serianu, 2018) are some of the most common cyberattacks facing many Kenyan organizations.

The 2019 sector statistics as reported by Communication Authority of Kenya (CAK) indicates that the past few years has particularly been tough for many Kenyan organizations regarding cybersecurity. There was a huge rise in cyber threat events targeting Kenyan businesses for the period between 1st July 2018 and 30th June 2019 and this situation has not got any better today. Table 1.1 below shows a summary of these cyberattacks' in numbers. In addition to these cyber threat events, cryptocurrency mining and software supply chain attacks are emerging cybersecurity threats that are causing devastating effect to many organizations across the world.

Table 1.1; Summary of cyberattacks between 1st July 2018 and 30th June 2019

Cyber Threats	Quarter 1	Quarter 2	Quarter 3	Quarter 4	Total
DoS/Botnets, malwares, web application attacks and system vulnerabilities	3,823,714	10,221,033	11,253,311	26,604,202	51,902,260

Extant literature indicates that a good number of cyberattacks arise from employee cybersecurity non-compliant behaviour. According to the 2017 data breach investigation report, 75% of cybersecurity breaches are caused by unauthorized outsiders(hackers) while 25% of the breaches arise from internal actors(insiders). Even with the 75% cybersecurity breaches due to hacking, the report goes further to point out that hackers thrive on user's risky security behavior to break into organization's computer systems. As such, the report found out that 66% of malwares attacks are installed as malicious attachment via staff emails; phishing being the most preferred social engineering means of attack. Highlighted also in the report is passwords handling. Password handling was underlined as a persistent security issue in most organizations with 80% of hacking-related breaches happening either due to stolen passwords and/or using passwords that are weak.

Globally, in year 2017 alone, the WannaCry ransomware attack wreaked havoc to more than 200,000 organizations in 150 countries, paralyzing critical computer related activities (Serianu, 2017). With ransomware attacks, hackers take control of a computer system and block access to it until some payments are made as ransom. Here, information resources were rendered unavailable and the perpetrators were unknown hackers. Locally, several high-profile security breaches have been witnessed that relates to cybersecurity. For

instance, it was reported by the world BBC news that on 22nd March 2017 a syndicate of cyber criminals consisting of insiders, hackers of Kenyan origin and international criminals hacked the Kenya Revenue Authority (KRA) systems. This led to a loss of about Kshs. 4 billion taxpayers' money with reports from the investigating authorities claiming that malwares were installed to access the attacked information systems. According to the Kenyan standard newspaper dated, February 8th, 2018, as happened on 7th October 2017, a Kenyan leading university online database was hacked, and examination results were altered using credentials of one of its staff. The same password had also been used to change exam details of two other students earlier. Here information integrity was compromised, and the organizational reputation was eroded. The leakage of about 1 TB of sensitive data from the ministry of foreign affairs is a good example relating to confidentiality of information. The ICT cabinet secretary, Mr. Mucheru, informed members of the public that hackers tricked some junior staff into changing their email password. It is from the click of the email and subsequent change of passwords that the hackers gained access to the ministry documents. These are just a few cases of the numerous security breaches that happens every day. Majority of companies do not disclose security breaches as they fear losing their customers trust and brand offering (CAK,2018). Increased focus on the human factors affecting cybersecurity in organizations is therefore of critical importance in dealing with the increasing tide of cyber-attack targeting organization's strategic assets.

The importance of SMEs to any nation cannot be underrated. UNDP (2015) relates contribution of SMEs to growth of economies, expansion of social structures and provision of employment opportunities. In terms of employment opportunities, the report mentioned that SMEs contributed approximately 84% employments opportunities in Kenya. Regarding provision of IS solutions for enabling operational efficiency in organizations, most sector of the economy relies on SMEs Information Technology (IT) companies for the provision and support of enterprise wide IS solutions. State-owned enterprises, financial services, manufacturing, hospitality & leisure, insurance, retail & consumer, transport & logistics and other sectors of the economy are largely dependent on IT based SMEs for provision of integrated IS solutions.

As compared to large organizations who have capability to adequately invest in cybersecurity measures, SMEs lacks adequate cyber defense controls in place and as a result, lacks capacity to effectively cope up with evolving cyber threats (Serianu, 2018).

When it comes to regulatory requirements, the 2019 Central Bank of Kenya (CBK) guidelines on cybersecurity for Payment Service Providers (PSPs) for example, is likely to present additional compliance pressure to PSPs including SMEs. In addition, with the enactment of Kenyan Data Protection Act 2019, different organizations are now likely to demand their technology providers to put in place an equal cybersecurity defense and data security norms as condition for acquisition and maintenance of IS solutions.

Owens & Onwubiko (2011) categorizes employee's security actions as either inadvertent or malicious when interacting with information resources. Employees are regarded malicious if they do not behave positively towards the implemented security control and considered as valuable assets, the first line of defense, when they contribute towards protection of information resources.

Current publications on cybersecurity culture associates terminologies such as robust cybersecurity culture, effective cybersecurity culture, desired cybersecurity culture, positive cybersecurity culture and healthy cybersecurity culture to favourable cybersecurity culture. A favourable cybersecurity culture is in place when employees in an organization becomes aware of their organization cybersecurity requirement(security awareness), complies with the security requirements of their organization as a natural aspect in their day to day activity (security compliant behavior) and where cybersecurity is everyone's responsibility(security ownership) (Tolah, Furnell & Papadaki, 2017) rather than the perception that cybersecurity issues belongs solely to the IT department or is someone's else responsibility. When favorable security culture is lacking, employees engage in undesired cybersecurity practice and this may lead to cybersecurity incidents. None the less, cultivation of a favourable cybersecurity culture in organizations, just like the organizational culture is dynamic and continuous process and cannot be realized in one day. It must be created, maintained and changed continuously (Roer, Petrič and Laycock, 2019) through appropriate strategies.

1.2 Problem Statement

The rapid adoption of ICTs by organizations the world over, has increasingly exposed information and non-information assets in organizations. There has been a constant stream of successful cyberattacks in recent past, and this has threatened the intended accrued benefits from ICTs adoption. A good number of studies have underlined human factors as

one of the root cause of cybersecurity incidents. A study by Kimwele et. al (2011), for example, revealed unauthorized disclosure of confidential information, deliberate systems attacks and copyright infringement as some of the security breaches suffered by Kenyan SMEs. Even more concerning, most organizations in Kenya do not have established cybersecurity training programs while documented Bring Your Own Device (BYOD) and Internet of Things (IoT) policies are also not in existent (Serianu, 2017). These findings signify unfavorable cybersecurity culture (ISACA/CMMI, 2018) in organizations.

Standard security frameworks and policies are useful to establish favorable cybersecurity cultures. However, standard cybersecurity frameworks such as ISO 27001:2013 have not found wide adoption among SMEs in Kenya while others available security frameworks provide only a limited view of the issues involved, and do not offer guidance on fostering security cultures. When it comes to security policies, most employees are known not to comply with ICT policies (Kimwele et. al, 2011; Kiveli, 2015), and this can lead to security incidents.

In addressing the human factors in cybersecurity management, research publications such as Van Niekerk & Reid (2014), ENISA (2017) and ISACA/CMMI (2018) have acknowledged implementation of robust cybersecurity culture in organizations. Despite many studies been conducted that relates to information security culture, their findings may not automatically apply to cybersecurity culture in SMEs in Kenya, since organizations operate within a particular industry with specific risk profile and are situated in different geographical locations (Alavi & Islam, 2013; Lessa & Gebrasilase, 2011). Key strategies for achieving favourable cybersecurity culture in SMEs in Kenya have also not been adequately studied.

1.3 Significance of the study

Many sectors across the industry depend on SMEs for provision of technological solutions that includes large enterprise IS solutions (enterprise wide IS solutions). SMEs offering enterprise wide IS solutions operate within a complex environment that is characterized by high adoption of cloud computing technologies, mobile based solutions and IoT. A diverse user's group including system developers, system administrators, subcontractors, temporary staff and interns, from these SMEs in many cases, connects to the client's enterprise computing systems remotely by use of various computing devices such as

personal computers. Also, the tech savvy capabilities of these employees allow then to bring with them smart devices such as smart watch that often connect to the enterprise network and thus increasing the cybersecurity attack vector. Based on the fact that SMEs offering IS based solutions do have many business linkages with large enterprises, the inadequate cybersecurity controls would make them a softer target to cyber criminals to advance cyber-attacks to large companies. This is more likely when employees in SME firm do not have or complies not with organizational cybersecurity security policies or do not receive regular cybersecurity education, awareness and training. Within the national context in Kenya, no high-level details have been provided on how healthy cybersecurity cultures can be established in SMEs. The resultant roadmap developed from this study can be used by cybersecurity practitioners to benchmark cybersecurity practices and processes in their effort to promote favourable cybersecurity culture in their organizations.

1.4 Research Objectives

1.4.1 Objective of the study

The study aimed to examine the human factors that impact on favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya and thereby identify a roadmap that can be used to enhance favourable cybersecurity culture in these SMEs.

1.4.2 Specific Objectives

i) To determine the effect of key human factors on favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.
ii) To identify an appropriate roadmap that can be used to enhance cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

1.5 Research Questions

i) What key human factors affect favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya?
ii) How do the key human factors in cybersecurity affect favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya?
iii) What human factors strategies should be developed in SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya to enhance the cybersecurity culture?

iv) How can SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya achieve a favourable cybersecurity culture?

1.6 Limitations of the Research

i) Certain information sought by the researcher could be confidential.
ii) Research cost was high since it included hiring of research assistants, and other requirements of the study like preparing the questionnaires.

1.7 Addressing the Research limitation

i) The researcher ensured that questionnaires carried no name of the respondents.
ii) The research was carried out within the available budget.

1.8 Basic Assumptions of the study

The following assumptions were made:

i) The respondent answered the questions asked correctly and truthfully.
ii) That the selected enterprise wide IS solution SMEs in Kenya availed all the data needed.

1.9 Definition of terms

Information Assets- Include information both in digital and analogue format as well as other components required to access, manipulate, store, transmit and share the data. Information is part of organizational strategic assets since many modern organizations relies on information for strategic advantage.

Enterprise wide Information Systems(IS) Solutions- Enterprise wide Information Systems(IS) solutions are computing data processing applications that enables organizations to integrate and coordinate their business processes in such a way that information can be shared across all functional levels and management hierarchies (Xu, 2016). There are best represented by large enterprise software solutions and any other integrated IS that are non-standalone applications.

Human Factors-Refers to the role(s) of human in cybersecurity. Also, it relates to humans as potential cyberattack target or unknowingly participating in cyberattacks.

Organizational Security culture- A general term for information security culture and cybersecurity culture in organization.

Small and Medium Enterprises (SMEs)- For this study, SMEs are organizations with employee between 10 and 250.

Tera byte (TB) A unit of measuring data adding up to 1000 GB

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

Securing organizational assets, both information and the non-information assets has become an increasingly critical requirement in modern organizations. Consequently, most organizations have instituted cybersecurity programs to manage cybersecurity matters. Effective management of cybersecurity in organizations goes beyond the mere implementation of technical cybersecurity solutions. Human factors in cybersecurity constitute the non-technical measures that are critical to cybersecurity management in organizations. With the skyrocketing numbers of cyber threats targeting organizations, existing literature on cybersecurity advocates for increased focus on the social ecosystem of cybersecurity in what is often referred to as cybersecurity culture. Building effective cybersecurity culture enables organizations to focus more on the human side of cybersecurity. For many organizations, cultivating a favourable cybersecurity culture remains work in progress (ISACA/CMMI, 2018) that requires appropriate implementation guidelines and support.

The subheadings outlined by this chapter include: An Overview of Cybersecurity, The Human Perspective of Cybersecurity in Organizations, Theoretical Framework, Cybersecurity Roadmaps, Key Human Factors in Cybersecurity Management and the Conceptual Framework. The source was from journals articles obtained from online research databases.

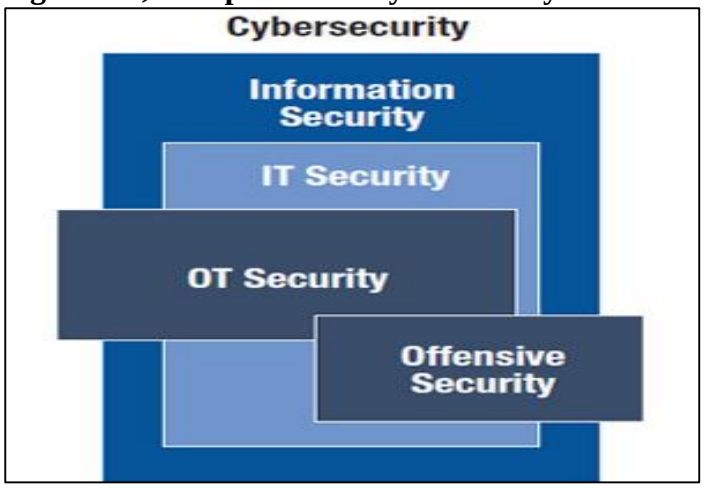
2.2 An Overview of Cybersecurity

The concept of cybersecurity was initially used in 1990s by scientists to refer to insecurity resulting from networked computers. On realization that threats arising from digital technologies could have a far-reaching impact to organizations, the scope was extended beyond mere technical view (Gong and Phibin, 2016), to accommodate other aspects that are of importance to cybersecurity management. Subsequently, cybersecurity terminology has often been used interchangeably with the term information security without much distinction. However, the two terms are not entirely analogous (ISACA, 2019) and it is therefore important to draw the distinction between them and clarify how they are related.

The international standard of information security, ISO/IEC 27000(2016), describes information security as safeguarding of information against unauthorized disclosure(confidentiality), unauthorized modification(integrity) and unauthorized access(availability). Other important properties related to security of information include authenticity (establishing the identity before granting permission), accountability (auditing transactions), non-repudiation (ability to prevent denial in electronic transactions) and reliability of information (Kamau et al., 2017).

The Kenyan cybersecurity strategy (2014) describes cybersecurity as the safeguard of ICT infrastructure, information and services from unapproved access, modification or destruction. Gartner (2013) distinction between cybersecurity and information security is much clearer. He views the two concepts as different yet closely related as shown in Figure 2.1 below.

Figure 2.1; Components of cybersecurity



Source: Isaca.org, 2019

This leads us to an understanding that cybersecurity in organizations is a much broader concept than surrounding concepts such as information security and aims to safeguard both information assets and the non-information assets against cyber threats. The strategic assets that cybersecurity strives to protect include the information resources that can be reached via the cyberspace, human who function in the cyberspace, and the cyberspace itself (Von Solms and Van Niekerk, 2013).

In modern organizations, the necessity for information security is being overtaken by cybersecurity (Rayne & Johan, 2014) since cybersecurity provides a much broader view in

safeguarding valuable organizational assets. Relating to cybersecurity, the global cybersecurity index is a multi-stakeholder initiative that assists countries to identify cybersecurity focus areas. The initiative also motivates countries to take actions aimed at improving their global rank on cybersecurity and in so doing, raise their overall commitment to cybersecurity initiatives (International Telecommunication Union, (2018)). According to the 2018 survey conducted by the International Telecommunication Union (2018), developed countries still top in the commitment to cybersecurity initiatives, with the United Kingdom leading the pack while United states of America and France followed closely at the second and third position respectively. Lithuania, Estonia, Singapore, Spain, Malaysia, Canada, Norway and Austria follow in that order respectively. Kenya ranks position 44 globally from that survey.

Reports from ICT industry clearly indicate the extent of socio-economic damage due to cyberattacks. In dealing with the cyberattack menace, most organizations have invested in modern cybersecurity technological solutions. However, technological solutions are not adequate by themselves, in protecting organizational assets effectively. In cognizance of this weakness, a good number of ICT industry players such as Serianu Cyber Threat Intelligence Team have called for an increased attention to the human side of cybersecurity in organizations. This study thereby, focused on cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

2.3 Human Perspective of Cybersecurity in Organizations

In search of appropriate measures for protecting information assets in organizations, security practices and techniques have progressed across various eras as underlined by a number of research publications. Zainudin (2017), makes reference to these eras by describing the four information security waves published by Von Solms(2006), popularly known as the first, second, third and the fourth information security waves. The first wave was technical, whereby security of information was regarded as a technical issue that was best handled by IT people. The second wave concerned management and entailed strong management participation and formulation of information security policies. The third wave, named as the institutionalization wave, came in from the period mid-1990s onwards and entails aspects such as information security culture. Information security governance is the fourth wave whereby top in command persons becomes individually answerable for all aspects relating to IT systems including information security they use for decision making.

Notably, these four waves of information security encompass the key aspects of information security namely, technological, human (people) and process aspects.

Martins and Da Veiga (2015) asserts that a combination of technological, people and process safeguards, all working together are essential elements for effective protection of valuable organizational assets. This assertion is echoed by Alhogail (2015) who informs that technological, people as well as other safeguards are important considerations in achieving a secure cyber environment in organizations. However, according to Karwowski and Glaspie (2018), most organizations tend to place more focus on technological and process aspect of securing information and with very little focus on the human factors. Even though technological solutions such as advanced intrusion prevention systems, firewalls, web filters, access control, authentication and authorization provides some level of protection against cyberattacks, this may not be adequate to deal with the human factors in cybersecurity, since humans are argued to be the weakest link in securing information in organizations; the very same way they can form the strongest link possible in cybersecurity management. One approach that work towards tapping human to a form the strongest link is establishment of favourable cybersecurity culture in organizations.

Information security culture and now cybersecurity culture is increasingly acknowledged as an effective approach in addressing the human factors in protection of valuable assets in organizations (Van Niekerk & Reid, 2014; ENISA, 2017; ISACA/CMMI, 2018). The close association between information security culture and cybersecurity culture necessitates reference on information security culture when discussing cybersecurity culture. Van Niekerk and Reid (2014) for example, adapted Von Solms & Van Niekerk definition on information security culture for cybersecurity culture. A more general description of cybersecurity culture is provided by Roer, Petrič and Laycock (2019) who relates security culture to "social behavior of a particular people that allow them to be free from danger or threats". When cybersecurity culture is institutionalized in organization, employees make information security requirements of their organization an intrinsic part of their daily work activities (ENISA, 2017).

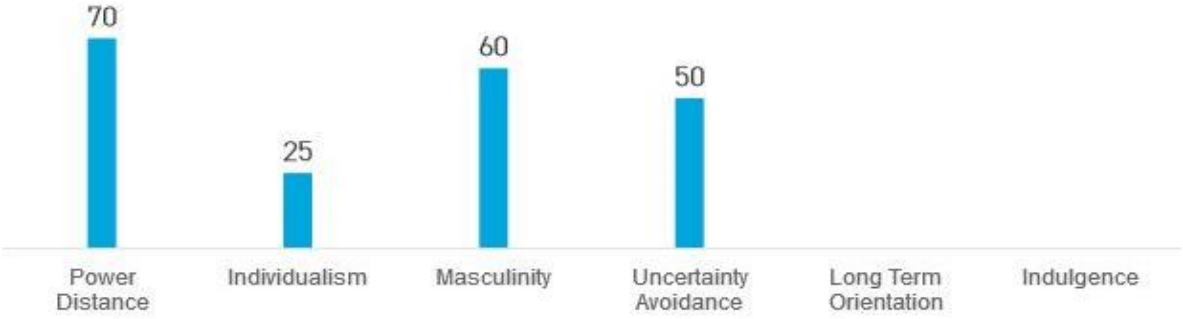
Cybersecurity culture can be analyzed at different levels of analysis including the individual, group, organizational and national level of analysis. National cybersecurity culture relates to a specific country while the organizational culture is associated with culture within a workplace setting. Scholarly works associated with Hofstede cultural value

framework relates to national culture and has been widely adopted in information security culture studies. Hofstede believes that an association exists between organizational culture and the national culture of any given country (Mohamed, 2016) and that security culture becomes embedded in the organizational culture(Martin & Da Veiga, 2017).

Hofstede-insights.com, provides some useful national cultural scores for various countries based on Hofstede framework six dimensions of culture. The six dimensions have been mentioned as: Individualism/collectivism, uncertainty avoidance, masculinity/femininity, power distance, long term/short term orientation and indulgence. The national scores take a value between 1 and 100, with 1 being the lowest and 100 being the highest. Every dimension is scored per country for comparison with other countries.

Kenya scores a relatively high score of 70 for power distance. The power distance being associated with the extent to which the less powerful individuals of an institution accept and expect that power is unequally distributed. This is illustrated by the extent to which clear lines of authority within a hierarchy are notable. As compared to other countries, the Latin America and Asian countries, African countries and the Arab have high power distance index scores. In terms of individualism/collectivism, the United States of America is one country with a higher scoring. The low score of 25 on individualism implies that Kenyan people are collectivist; motivated to doing things for their group than for themselves and having close ties with other individuals in the group. A masculine culture is one that is competitive and that strives for achievements, heroism and material rewards for success. Kenyan culture measures high on masculinity dimension with a score of 60. Uncertainty avoidance is the situation whereby societies feels comfortable or uncomfortable to unstructured circumstance. Countries with high uncertainty avoidance ranking tend to put in place strict laws and rules as compared to societies with low uncertainty index. The intermediate score of 50 in uncertainty avoidance indicates that Kenya has no clear preference in this dimension. The country comparison tool does not provide the scoring on long term orientation and indulgence dimensions.

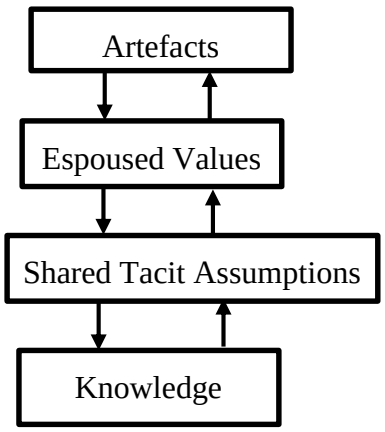
Figure 2.2; Scores relating to security culture in Kenya



Source: Hofstede insights.com, 2020

Other scholarly works such as Schein 1999 organizational culture model do not consider the interrelation between the national culture and organizational culture. They argue that organizations develop their own culture that is different from national culture, to make them more competitive. The 1999 Schein organizational culture model, as it is widely known, is quite popular in research when it comes to understanding cultures in organizations. This model was originally developed by Edger Schein to bring about understanding of culture in organization by illustrating three levels culture that includes: Artefacts, Espoused values and Shared assumptions. Schein model has been improved by researchers in information security culture by including a fourth culture level of knowledge. Subsequently, the resulting four tier model has become popular in information security and now in cybersecurity studies to describe the contribution of culture in security management (Reid & Van Niekerk, 2014). Artefacts (observable behavior), Espoused values (official behavior), shared assumptions (employee real behavior) and Security knowledge are thus the four culture layers relating to cybersecurity culture in organizations (Reid & Van Niekerk, 2014).

Figure 2.3; Components levels of cybersecurity culture in organizations



Derived from Reid & Van Niekerk (2014)

Artefacts are the physical representation of culture. This level of culture includes the visible organizational structure and processes (Van Niekerk & Reid, 2014) that manifest the observable security behavior of employees. To attain the desired culture at this level, employees requires appropriate skills to perform their security related tasks correctly and securely (Von Solm & Van Niekerk, 2006). Examples of security elements at the artefact level as reported by Zainudin (2017) are visual personnel security (such as clothing and badges), physical environment (such as physical office layout, open or partitioned office space, security appliances and security technologies) and visible and audible behavior patterns in an organization (such as norms, ceremonies, slogans, rituals, symbols and rites).

Espoused values are the security goals, philosophies and principles regarded to have some inherent value to members of an organization. They represent the official security viewpoints of an organization (Von Solms & Van Niekerk, 2010) and indicates the official security behavior that employees should follow to achieve operation goal of the organization (Zainudin, 2017). Security elements relating to espoused values are information security confidentiality, integrity and availability (Zainudin, 2017).

Shared tacit assumptions is a deeper layer of culture that represent employees' real security behavior. Examples of cybersecurity culture elements that may develop culture at this level are reward and punishment, assignment of security roles and responsibilities and peer relationships *(*Zainudin, 2017*).* Organizations must therefore strive to develop positive shared tacit assumptions in employees to ensure success in security goals.

Security culture should take into account security knowledge as the fourth level of culture in enhancing the understanding of the security culture in organizations (Van Niekerk & Reid ,2014; Von Solm & Van Niekerk, 2006). The authors interpreted that for security culture to be embedded as a subculture of the overall organization culture, all activities in the organizations need to be performed securely. Knowledge is therefore modelled as an additional culture level to ease the understanding of the effect of knowledge on the overall information security culture (Von Solm & Van Niekerk, 2006).

The resultant model illustrates that the overall cybersecurity culture (observable cybersecurity culture) in any organization is the accumulative effect of each underlying layers of culture where each layer influences the overall cybersecurity efforts either positively or negatively. According to Von Solms's & Van Niekerk(2006), shared tacit

assumptions would for example influence on how individuals interpret cybersecurity polices and implement security procedures, representing espoused values of the organization, and this in turn determines the observable cybersecurity culture. Security knowledge is required at each level of the cybersecurity culture model. For instance, at the artefact level, users need adequate knowledge on how to carry out their day to day tasks securely. Adequate knowledge of what to include in security policies is needed by the team preparing the security policy for the policies to be useful in an organization. Where the beliefs of the user's do not resonate with the espoused values of the organization, understanding why a specific control exists is crucial to help in ensuring that employee complies to the required security practices. Likewise, the artefact layer can influence the espouse values of the organization which in turn influences employee shared tacit assumptions.

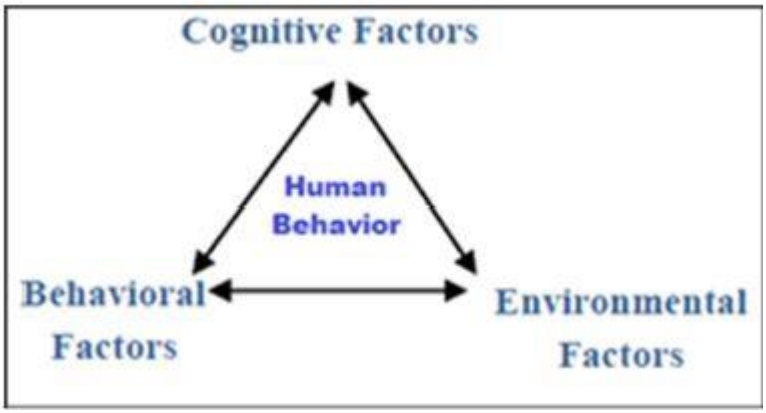
Research, for example Roer, Petrič and Laycock (2019) has presented the measures of security culture as attitudes, behaviour, cognition, compliance, responsibilities and norms. These dimensions correspond closely to the four levels of cybersecurity culture. In their white paper, they illustrate a toolkit for evaluating security culture in organizations built from the above-named measures of security culture. Even so, only few empirical studies have been undertaken on developing and implementing of favourable cybersecurity culture in organizations.

2.4 Theoretical Framework

2.4.1 The Social Cognitive Theory(SCT)

The SCT was developed by Albert Bandura from the mid 1970 onwards. Over the years, the theory has been widely utilized in research across several domains including information systems, information security and so forth (Raeside, Hall & Middleton, 2018). In their research work, Gupta, Sharman and Ada (2009) highlighted that the framework provided by SCT is very important in terms of understanding, predicting and changing human behavior in organizations. An illustration of the framework provided by SCT is shown in Figure 2.4.

Figure 2.4; Framework of SCT



Source: Bakry, Mirza & Alhogail(2015).

According to Bandura (2001), people acquire and maintain certain behavioral patterns in organizations in terms of triadic reciprocal causation. Triadic reciprocal causation is a concept referring to the reciprocal nature of interaction among personal factors (inform of cognitive and other personal factors), environmental factors and behavioural factors of the SCT. These three set of factors interplay, interact and bear influence on one another to form a causal model of triadic reciprocity. Behavioral and cognitive factors relate to individuals including when in the workplace setting. These two sets of factors play an important part on how employee behave in the workplace. The behavioral factors in SCT constitute knowledge acquisition through new ideas and practice (Godwin and Verdin, 2019) while the cognitive and other personal factors relate to the quality of analytic thinking and expected outcomes to name just a few (Godwin and Verdin, 2019). Environmental factors on the other hand relate to organizations and other external influences that exert pressure on an organization from its external environment. The SCT distinguishes three types of environmental structures, environments that are imposed, selected and constructed. Imposed environments may include situations an individual must interact with on a daily basis such as the workplace (Bandura, 2001) and this is the environment considered by this study. All the three set of factors operate as interacting determinants and influence one another bidirectional in regulating human security behavioral patterns in organizations and in establishing security culture level in organizations.

Da Viega and Eloff (2008) illustrated establishment of information security culture in organizations by developing an all-inclusive information security framework. They categorized the various information security framework components into individual, group

and organizational tiers and described regarding information security culture cultivation in organizations. Their study illustrated how implementation of appropriate information security controls in organizations would influence information security behavior in organizations which in turn would cultivate a positive information security culture.

Several studies in literature have used SCT (Gupta, Sharman & Ada, 2009). Barky, Mirza and Alhogail (2015), for example, applied the SCT to develop the information security human factors diamond framework. Their framework identified human factors that can influence information security behavior of members in organizations. The study further related these human factors to the three main factors of SCT in the development of the information security framework. The identified mechanisms for influencing employee security behavior of their study were consistent with those identified by Da Viega and Martins (2015). Agarwal et al (2013) further demonstrated the applicability of the SCT in information systems discipline. In their study, they considered organizational factors, technological factors and individual factors from a SCT perspective. The usefulness of the SCT has also been confirmed by Rana and Dwivedi (2015) who employed the extended SCT to understand the adoption of an electronic government system.

The findings of these studies, however, may not automatically apply to cybersecurity culture in SMEs in Kenya since organizations operate within a particular industry that have a specific risk profile and are situated in different geographical locations (Alavi & Islam, 2013; Lessa & Gebrasilase, 2011).

2.5 Cybersecurity Roadmaps

The international Energy Agency (2014) when developing their strategic roadmap referred to roadmaps as plans of strategic nature that specify tasks an organization need to carry out to achieve stated goals and outcomes over defined time spans. They recommended that successful roadmap should identify priorities, milestones, obstacles, gaps, action items in addition to the roadmap goals and timelines. To achieve desired cybersecurity culture, different organizations adopt various approaches and techniques as cybersecurity roadmaps. These approaches and techniques are diverse in nature and to achieve the outlined cybersecurity goals, SMEs need cybersecurity solutions optimized to their business environment and available resources.

Standard security frameworks and policies relating to cybersecurity are useful to establish favorable cybersecurity cultures; however, according to the 2018 International Organization for Standardization(ISO) survey, these security frameworks have not found wide adoption in Kenyan SMEs. The survey indicates a total of only 31,910 certified organizations in ISO 27001:2013 globally and this is a gradual decline from 39,501 for year the 2017 according to a similar study conducted by ISO. Locally, Kenya had only 7 certified organizations in this standard which was a drop from 11 organizations the previous year. Only a few studies have examined the factors inhibiting wide adoption of standard security standards. Among the reasons cited by Khan et.al (2011) for slow adoption and certification of ISO 27001:2013 in organizations are inexperienced ISO implementation team, change management issues and low understanding of the standard. Implementation of other global standard security frameworks such as NIST (2018) and COBIT (2011) has also not been easy particularly for SMEs due to the fact that these SMEs face similar challenges as large companies. Regarding security policies, most employees are known not to abide by security policies (Kimwele et. al, 2011; Kiveli, 2015), and this can lead to security incidents.

Establishment of supportive cybersecurity culture within organizations can result in reduction of cybersecurity incidents when employees clearly understands the cybersecurity requirements of the organization's and thus behave positively towards the implemented security control as part of their daily work routine. A cybersecurity culture that supports the outlined cybersecurity initiatives would pave way for certification of organizations on security standards. Reduced cyber incidents, capability to resume business operations after cyberattack, increased understanding of potential cyber threats and customers trust in company's brand offerings are some of the well-known benefits of implementing an effective cybersecurity culture in organizations (ISACA/CMMI, 2018).

2.6 Review of Empirical studies

The 2018 global cybersecurity study conducted by ISACA/CMMI relates to cybersecurity culture. This study discovered that significant gap existed between the desired cybersecurity culture and the current cybersecurity culture in many organizations they studied. Out of the 4,815 organizations that were studied, 32% had significant cybersecurity culture gap and only 5% of organizations attested to have no cybersecurity culture gaps. Domestically, research, for example Kimwele *et. al,* (2011), outlined some undesired security practices in Kenyan SMEs. Unauthorized disclosure of confidential information,

deliberate attack on organizational systems though malicious deleting, corrupting or exposing sensitive data, download and install of infringing copyright materials and inadequate backups not been performed are some of the undesired security practices outlined. Other notable undesired cybersecurity practices common in organizations include sharing of access passwords among employees and access to online platforms that may pose danger to organization's assets (Alam et. al, 2017). Organizations with unfavourable cybersecurity culture tend to be vulnerable to cyber breaches and data loss, susceptible to regulatory penalties, loss of customer trust and thus missed business opportunities (ISACA/CMMI, 2018).

A good number of studies such as Areej(2015); Tolah et al(2017); Martins & Da Veiga(2015); AlHogail & Mirza(2014); Sherif et al(2015) have acknowledged adoption of information security culture as an effective solution to address risky human security behavior in organizations. Information security been part of cybersecurity (Gartner, 2013) necessitates reference to be made on information security culture when discussing cybersecurity culture (Van Niekerk & Reid, 2014) within an organizational context.

In investigating mechanisms for influencing information security culture, Da veiga & Martins (2015), established that compliance to information security requirements, security policy, management commitment and security awareness have a positive influence on information security culture in organizations. This was achieved by validating a model of these four information security culture mechanisms with a structural equation modelling technique using empirical data derived from Information Security Cultural Assessment instrument. Research findings by Alhogail, Mirza & Bakry (2015) are very consistent with the foregoing findings. Alhogail, Mirza & Bakry (2015) on the other hand considered two dimensions in their human factor diamond framework; the employee and organization dimensions. They adopted a survey of expert views research method which confirmed that human security behavior in organization is influenced by the following human factors; security policy, management practices, security communication, national & organization security culture, standards & regulations, security training & awareness, change of old practices, acceptance of responsibilities, monitoring & control, reward & deterrence. Their research framework has been advanced in subsequent studies to a wider scope. The foregoing human factors are also congruent with a more recent review of human factor by Karwowski & Glaspie(2018) that identified attitude & involvement, incentives &

deterrence, security policy, awareness & training and management support as key human factors appropriate to enhace information security culture in organizations.

Other factors and issues that have been identified to shape employee security behavior include risk assessment, IS education & training, knowledge acquisition, employee soft issues(such as ethics, etiquette, personality traits) and workplace capabilities such as employee competence, job satisfaction, reliance on temporary employees, effectiveness of security monitoring procedure, reward and disciplinary procedure and security practices(Da veiga & Martins, 2017; Tolah, Furnell & Papadaki, 2017).

2.6.1 Synthesis of key Human Factors Relating to Cybersecurity in Organizations

Based on the human factors highlighted above and the proceeding discussion on security cultural research frameworks, key human factors were identified that could influence favourable cybersecurity culture in SMEs providing enterprise wide IS solutions. In line with the social cognitive framework utilized by Alhogail, Mirza & Bakary(2015), this study identifies Top management support and involvement to cybersecurity program, Cybersecurity policies, Cybersecurity training and awareness programs, Compliance with cybersecurity Legal and regulatory requirements, Cybersecurity monitoring and audit, Reward and Deterrence measures and Cybersecurity change management as the key human factors that impact on favourable cybersecurity culture in organizations being studied. The framework thinks about the key human factors adopted from table 2.1 as the appropriate cybersecurity controls that all working together will lead to favourable cybersecurity culture in SMEs in Kenya that providing enterprise wide IS solutions. The remaining section entails operational definition of variables utilized by the study while the operationalization regarding these study variables is captured in table 2.2 below.

Table 2.1; Synthesized key human factors for cybersecurityculture in organizations

#	**Key human factors in cybersecurity management**	**Referenced research study**
1	Top management support and involvement to cybersecurity program	Alhogail, mirza & barkary (2015), Martins & Da Veiga(2015), Nelson, Chan & Alnatheer(2012), Karwowski & Glaspie(2018)
2	Cybersecurity policies	Karwowski & Glaspie(2018), Alhogail, mirza & barkary (2015),Tolah, Furnell & Papadaki(2017), Martins & Da Veiga(2015), Nelson, Chan & Alnatheer(2012)

3	Cybersecurity training and awareness programs	Tolah, Furnell & Papadaki(2017), Martins & Da Veiga(2015), Tolah, Furnell & Papadaki(2017), Giannakopoulos et al(2015)
4	Compliance with cybersecurity Legal and regulatory requirements	Martins & Da Veiga(2017), Al-Kalbani(2017), Tolah, Furnell & Papadaki(2017)
5	Cybersecurity monitoring and audit	Alhogail, Mirza & Bakary(2015)
6	Reward and Deterrence	Alhogail, mirza & barkary (2015), Martins & Da Veiga(2017); Karwowski & Glaspie(2018)
7	Cybersecurity change management	Alhogail, mirza & barkary (2015)

Management support is an important human factor in formation of desired cybersecurity culture in organizations. Top management entails provision of supportive environment for cybersecurity culture by offering a strong and consistent support (Karwowski & Glaspie, 2018) in terms of allocating adequate financial and material resources to the cybersecurity program. Material resources include among other initiatives, provision of appropriate cybersecurity reporting structures to support cybersecurity issues in organizations, so that everyone is conversant with the current cybersecurity issues facing the organization. Top management consistent support also extends to provision of leadership by example (Zainudin, 2017) relating to cybersecurity initiatives undertaken by the organization.

Cybersecurity policy is a foundational element of any cybersecurity program. Security policies and policy guidelines directs cybersecurity culture and form the basis for creating shared beliefs and values in organizations (Martins & Da Veiga, 2015). Cybersecurity policy is useful in organization when it is well enforced. Top management should therefore ensure enforcement of cybersecurity policies & procedures in the organization. To increase employee willingness to comply with defined cybersecurity rules and procedures, management need to provide employee with a clear understanding of the policy statements and guideline. As such, cybersecurity policy needs to be well communicated to all employees frequently and crafted in a language that is easily understood by every employee.

Organizations need to institute an awareness programs relating to cybersecurity designed to provide the workforce with an understanding of the cyber risks and relevant controls to use and abide by in organization. New employees should receive cybersecurity awareness program during employee induction process (ISO 27001:2013). Existing employee should also be offered frequent cybersecurity training and awareness programs to enable them keep abreast with emerging cyber threats. Education and training programs are conducted

within classrooms environment to give employees the skills required to perform cybersecurity roles and responsibilities. Martins & Da Veiga(2015) attests that frequent training and awareness programs have been established to have some positive impact on the information security culture.

Most organizations are mandated to comply with some sort of mandatory cybersecurity requirements by regulatory authorities. The 2019 Central Bank of Kenya guidelines on cybersecurity for example, is one such compliance requirement. These guidelines outline several requirements that may be difficult to achieve without an effective culture of cybersecurity in place in organizations. In addition, the recent enactment of Kenyan data protection Act 2019 is likely to push organizations to demand their technology providers to put in place an equal cybersecurity defense and acceptable data security norms.

Cybersecurity change management initiatives are required to provide guidance to equip and support organizations move from their current cybersecurity status to the desired cybersecurity state. Information security culture change principles suggested by Alhogail (2015) relevant and applicable for this study are user involvement in cybersecurity initiatives, effective communication on cybersecurity across organizations and appointment of change agents or champions to spearhead cybersecurity initiatives within organization.

Several theories such as theory of planned behaviour and protection motivation theory have been used to understand and explain user intended action relating to compliance with organizational security requirements. Policies need to define a clear course of actions to be undertaken for non-complying employee. Employees are likely to engage in risky behaviour in organizations in absence of clear and consistent consequences for noncompliance. Employee who complies with the defined rules and requirements need to be motivated to encourage them keep on abiding with the outlined cybersecurity requirements.

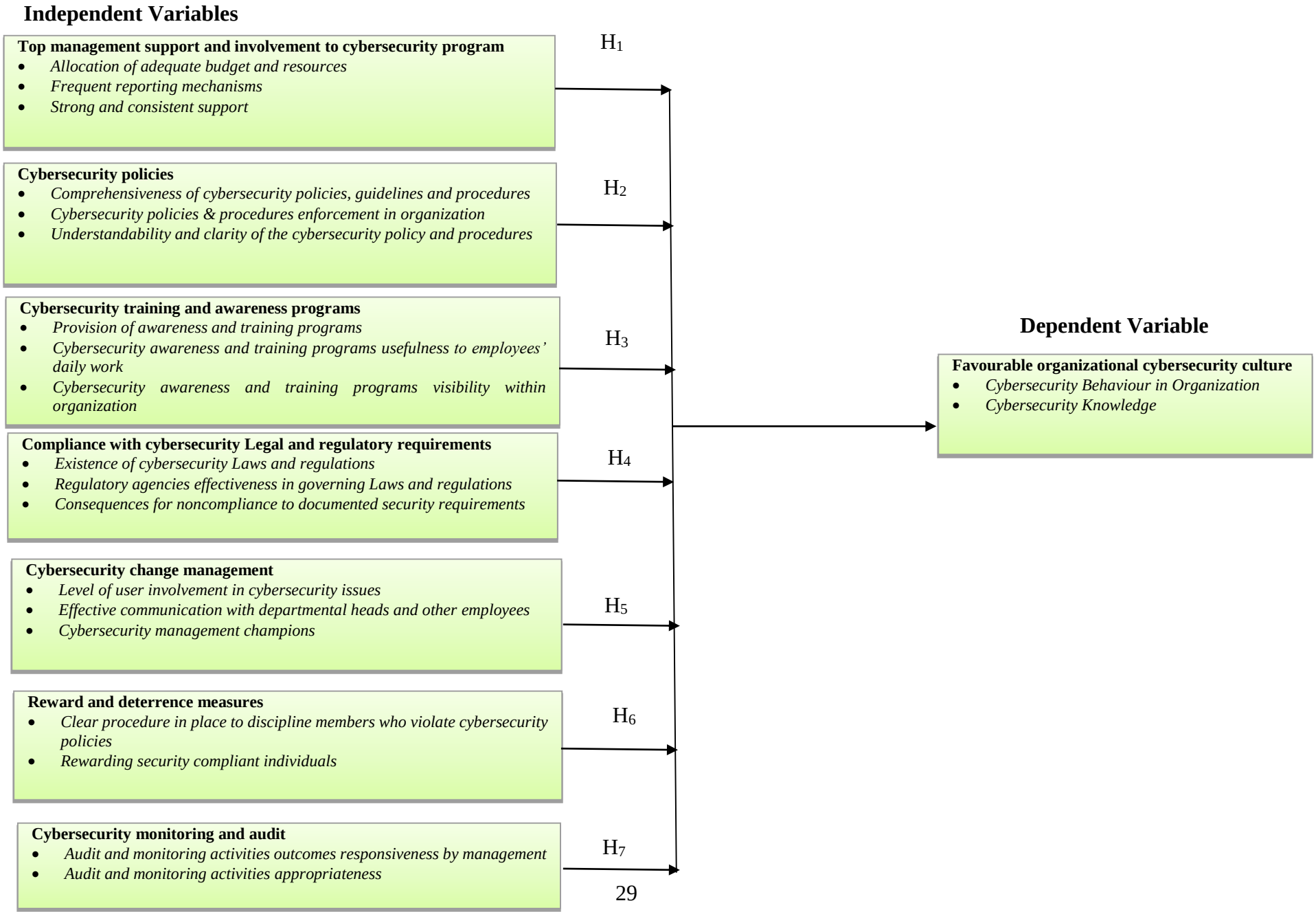
Cybersecurity audit and monitoring has also been identified as a viable mechanism for influencing favourable cybersecurity behaviour (Al-Kalbani, 2017). Organizations therefore need to conduct monitoring activities for their ICT systems and employees' activities. Frequent vulnerability assessment and penetration testing provide useful audit

reports on weak areas that may be exploited to perpetrate cyberattacks. Management need to take appropriate actions as informed by be audit reports.

2.7 Conceptual Framework

The framework provided by SCT was chosen for its ability to accommodates all the human factors we identified as being critical to enhance favourable cybersecurity culture in the organizations. Cognitive factors & behavioural factors dimensions of the social cognitive framework relate to the workforce while the environmental factors relate to organization itself. The cognitive & behaviour factors were addressed by cybersecurity training and awareness programs, cybersecurity monitoring and audit, reward and deterrence measures while environmental factors were covered under cybersecurity policies, top management support and involvement to cybersecurity program, cybersecurity change management, compliance with cybersecurity Legal and regulatory requirements. These constituted the independent study variables. The dependent variable was expressed by cybersecurity behaviour in organization and cybersecurity knowledge. The conceptual framework was then used to guide the research methodology.

Figure 2.5; Conceptual Framework



Source, Author (2019)

Study hypotheses

The study tested the following hypothesis:

H_1 Top management support and involvement to cybersecurity program has a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

H_2 Cybersecurity policies have a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

H_3 Cybersecurity training and awareness programs have a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

H_4 Compliance with cybersecurity Legal and regulatory requirements have a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

H_5 Cybersecurity change management has a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

H_6 Reward and deterrence measures have a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

H_7 Cybersecurity monitoring and audit has a positive effect on favourable organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

Table 2.2; Operationalization of the study variables

Variables		**Indicators**
Independent Variables	**Top management support and involvement to cybersecurity program**	• *Allocation of adequate budget and other resources* • *Frequent reporting mechanisms* • *Strong and consistent support by management*
	Cybersecurity policies	• *Comprehensiveness of cybersecurity policies, guidelines and procedures* • *Cybersecurity policies & procedures enforcement in organization* • *Understandability and clarity of the cybersecurity policy and procedures*

	Cybersecurity training and awareness programs	• *Provision of awareness and training programs* • *Cybersecurity awareness and training programs usefulness to employees' daily work* • *Cybersecurity awareness and training programs visibility within organization*
	Compliance with cybersecurity Legal and regulatory requirements	• *Existence of cybersecurity Laws and regulations* • *Regulatory agencies effectiveness in governing Laws and regulations* • *Consequences for noncompliance to documented security requirements*
	Cybersecurity change management	• *Level of user involvement in cybersecurity issues* • *Effective communication with departmental heads and other employees* • *Cybersecurity management champions*
	Reward and deterrence measures	• *Clear procedure in place to discipline members who violate cybersecurity policies* • *Rewarding security compliant individuals*
	Cybersecurity monitoring and audit	• *Audit and monitoring activities outcomes responsiveness by management* • *Audit and monitoring activities appropriateness*
Dependent Variable	**Favourable organizational cybersecurity culture**	***Cybersecurity Behaviour in Organization*** • *Availability of physical cybersecurity products, visual personnel security, and audible & visible behavioural patterns in the organization* • *Desirability for cybersecurity confidentiality, integrity and availability in organization* • *Employee attitude towards cybersecurity initiatives*
		Cybersecurity Knowledge • *Employee knowledge on how to carry out their day to day tasks securely* • *Knowledge on cybersecurity policy contents in addressing the cybersecurity requirement of the organization* • *Knowledge on cybersecurity topics to address the security requirement of the organization*

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

The sub headings covered in this chapter include: Research design, Target population of the study, Sample size and sampling procedure, Data collection instrument, Validity and reliability, Data analysis techniques and Ethical considerations.

3.2 Research Design

According to Singh (2006), research design entails: research strategy, choice of research tools, sampling design and choice of statistical techniques. A quantitative research strategy inform of descriptive research design was deployed to obtain information relating to the status of the current situation that concerned the topic in question. The design was chosen because the study purposed to describe things as they were at the time of the study rather than manipulating the study variables. Mail survey method was adopted to gather primary data. The mail survey adopted questionnaires as data collection tool that were sent over the emails to the target organizations and administered to the respondents through the assistance of a contact person in the organizations.

3.3 Target Population of the Study

The study population comprised of the companies offering IT related systems and services as per the official 2019 yellow pages' Kenya online directory. The researcher used three criteria to select the target population of the study from the computer-software & services category, information and communication technology services category and software developers' business category of the yellow pages' directory. The selection criteria included SMEs that were premised solely in Nairobi City County, that provides enterprise wide IS solutions and that had active websites. The study identified 34 SMEs as providing enterprise wide IS solutions within the geographical region considered. This constituted the target population.

3.4 Sample Size and Sampling Procedure

For the sample size, all the 34 SMEs identified as providing enterprise wide IS solutions were considered by the study. Judgemental sampling was utilized to choose respondents from these SMEs that were believed to have the required information relating to the

research problem.The respondents comprised of a senior personnel who is responsible for cybersecurity issues, the ICT head, technical ICT staff and a general user of ICTs of the selected SMEs. This aided in understanding the current status of cybersecurity practices and the desired cybersecurity culture in these institutions. The illustration of the respondents is as in Table 3.1

Table 3.1; Total Number of Respondents in identified SMEs

%	Respondents for the study per org.	Representation
1	Senior personnel responsible for cybersecurity issues	1
2	ICT head	1
3	Technical ICT staff	1
4	General user of ICTs	1
	Total number of respondents in selected SMEs is 4*34	**136**

3.5 Data Collection Instrument

Primary data and secondary data were utilized. A structured questionnaire was used for the collection of the primary data. In each of the identified SMEs, a contact person assisted in administration of questionnaires in accordance with table 3.1 above so as to collect data regarding the general information of the respondents and information relating to cybersecurity culture in the selected SMEs. The questionnaire was designed to collect quantitative data where closed-ended questions provided more structured responses that ensured accurate and uniform collection of quantitative data. The questionnaire sought to determine respondent's opinions as to what is considered as the key human factors that affect favourable cybersecurity culture in their organizations. It also collected data on Top management support and involvement to cybersecurity program, Cybersecurity policies, Cybersecurity training and awareness programs, Compliance with cybersecurity Legal and regulatory requirements, Cybersecurity monitoring and audit, Reward and Deterrence measures and Cybersecurity change management regarding establishment of favourable cybersecurity culture in their organizations. For the secondary data, a review of existing document was done during literature review. Documents sourced from online journals, international publications and the internet data were used to gather data on cybersecurity topics and cybersecurity frameworks. This formed the secondary data that assisted in choosing relevant indicators for the research instrument.

3.6 Validity and Reliability

Content validity was employed by this study as a measure of the extent to which the data collected through data collection tool represented the concept being measured. The developed questionnaire was scrutinized by an experienced researcher and a PhD student for content validity before it could be administered. To assess the reliability of data collected using the research instrument, a pilot study was carried out. In the pilot study, the test-retest method of assessing reliability was done where the same questionnaire was administered to the same group of individuals at two separate times. All questionnaires that were administered the second time had similar response as those administered the first time and this proved that the questionnaires were reliable hence appropriate for use in the study. Some questions provided more information about the topic under investigation and this ensured determination of consistency in the responses given. The email contacts of organizations identified for the study were consolidated and a cover letter regarding the purpose of research together with the questionnaire was then submitted through the official email addresses of the organizations. Later, several follow-ups were done with the key contact individuals and this was mainly done through emails and phone calls.

3.7 Data Analysis Techniques

A thorough check was done on the completed questionnaires after the data collection and before coding and entering the data in SPSS version 23 for analysis. The thorough check on the questionnaire's responses was done to identify and note any possible errors and omission. Data was analyzed using descriptive and inferential statistics techniques that took care of the quantitative data gathered during the study. The descriptive statistics included standard deviations, means, frequencies and percentages while inferential statistics entailed correlation and multiple regression analysis. The multiple regression analysis consisted the model summary, analysis of variance (ANOVA) and regression coefficient. The multiple regressions determined the relative importance of each human factor (independent variable) with respect to the favourable cybersecurity culture (dependent variable) and this was determined by the regression coefficients. Correlation analysis determined whether any association existed between the study variables and determination of the nature of the relationships (ie whether positive or negative relationship). A measured of whether any statistical significance difference existed between the means of independent groups was achieved from ANOVA results findings.

The multiple linear regression analysis as expressed as follows

$$Y= \alpha + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 \ldots\ldots\ldots\ldots + \beta_n X_n + \varepsilon$$

Where;

Y = Favourable Cybersecurity Culture

X_1= Top management support and involvement to cybersecurity program, X_2= Cybersecurity policies, X_3= Cybersecurity training and awareness programs, X_4= Compliance with cybersecurity Legal and regulatory requirements, X_5= Cybersecurity monitoring and audit, X_6= Reward and Deterrence measures, X_7= Cybersecurity change management

β_1, β_2 and β_3 are independent variables regression coefficient

ε = is unexplained variance errors term

3.8 Ethical Considerations

First the researcher sought permission from the management of target organization before collecting data. The researcher also held a moral obligation to only use the information given exclusively for intended research work. This was emphasized in the cover letter that accompanied the questionnaire in reassuring the respondents of the use and confidentiality of their information.

CHAPTER FOUR

4.0 DATA ANALYSIS FINDINGS AND DISCUSSION OF THE FINDINGS

4.1 Introduction

Areas presented in this chapter include: Analysis of research data, the research findings, and research findings discussion. The findings are presented in accordance with the research methodology and research objectives, so that research questions are answered. The results findings contain results on demographic characteristics, descriptive analysis, and inferential statistics. The findings presentation is in tabular form. The study was carried out in the 34 identified SMEs. In each of the identified SME, one senior personnel responsible for cybersecurity issues, the ICT head of department, a technical ICT staff and one general user of ICTs were requested to provide their views, perceptions, and opinions regarding cybersecurity culture in their organization.

4.2 Response Rate

A total of 136 questionnaires were issued out to the target SMEs. 72 questionnaires were submitted back as responses and this implied a 53% response rate which the researcher considered adequate to make recommendations and conclusion of the study. For descriptive research, Mugenda and Mugenda (2003) argues that a response rate of 50% is considered adequate for data analysis. Based on this assertion, the received threshold was considered sufficient for analysis.

Table 4.1; The Response Rate

Response Rate	Frequency	Percent (%)
Questionnaires that were filled and returned	72	53%
Questionnaires that were un submitted	64	47%
Total	**136**	**100**

Source: Research Data (2020)

4.3 Demographics

The gender, age group, highest educational level, job position of the respondents and number of years the respondent had worked in their organization demographics was sought for.

4.3.1 Gender of the Respondents

Out of 72 responses, 75% (54) were completed by male while 25% (18) by female. These findings imply that SMEs that offers enterprise wide IS solutions are dominated by male employees. These finding also support those of Gbedomon (2016) who argued that there a need for supporting women access to ICT in Africa for inclusivity in economic development.

Table 4.2; The Gender of the Respondents

		Frequency	Percent
Gender	Male	54	75.0
	Female	18	25.0
	Total	72	100.0

Source: Research Data (2020)

4.3.2 Age Group of the Respondents

In terms of the respondents age groups, the results show that 40.3% were in the category 26 to 35 years, 20.8% were in 18 to 25 years' category, 31.9% were in 36 and 45 years while 6.9% were above 46 years. These findings imply that SMEs that offers enterprise wide IS solutions are dominated by young employees who are energetic, versatile, and able to cope with rapid technological advancement.

Table 4.3; The Age Group of the Respondents

		Frequency	Percent
Which of these age groups (Years) are you in	18 to 25 years	15	20.8
	26 to 35 years	29	40.3
	36 to 45 years	23	31.9
	46 or more years	5	6.9
	Total	72	100

Source: Research Data (2020)

4.3.3 Highest Educational Level of the Respondents

For the respondent's highest educational level, 18.1% had postgraduate degrees as their highest-level of education, 58.3% had undergraduate degrees and 23.6% had diplomas as illustrated by Table 4.4. This is an indication that all the respondents were highly educated to meet the technical demands of the job requirements they undertake in their respective firms.

Table 4.4; Highest Educational Level

		Frequency	Percent
Highest educational level	Diploma	17	23.6
	Undergraduate degree	42	58.3
	Postgraduate degree	13	18.1
	Total	72	100

Source: Research Data (2020)

4.3.4 Job Positions

The research sample was a representative of all the levels of the organization structures and thus included the key staffs across organization. 15.3% of the responses were from ICT department heads, 45.8% were technical ICT staff, 23.6% were general users of ICTs and 15.3% were senior personnel responsible for cybersecurity matters as illustrated in Table 4.5.

Table 4.5; Respondents Job Description

		Frequency	Percent
Hierarchical level of your job description	Senior personnel responsible for cybersecurity matters	11	15.3
	ICT head department	11	15.3
	Technical ICT staff	33	45.8
	General user of ICTs	17	23.6
	Total	72	100

Source: Research Data (2020)

4.3.5 Respondents Working Experience

Table 4.6 instances that 29.2% of the respondent had worked over 5 years, 41.7% had worked between 2-3 years, 12.5% had worked 4-5 years while 16.7% had worked for less than 1 year in their current organization. These findings show that the study involved employees with different working experience in their current workplace hence a diversity in the responses received.

Table 4.6; Respondents Working Experience

	Category	Frequency	Percent
How many years have you worked with your organization	0-1	12	16.7
	2-3	30	41.7
	4-5	9	12.5
	Over 5	21	29.2
	Total	**72**	**100**

Source: Research Data (2020)

4.3 Descriptive Analysis

Responses received were analysed using standard deviation (std Dev), mean and percentages.

4.4.1 Key Human Factors Affecting Favourable Cybersecurity Culture

The researcher sought to establish human factors strategies that the respondents supposed to have influenced cybersecurity behaviour in their organizations with a view of relating to findings from empirical studies. The respondents were asked to respond to a number of human factors strategies outlined in the data collection instrument as to whether they believed these strategies have or have not influenced cybersecurity behaviour in their organizations. Most of respondents as table 4.7 shows, agreed that Top management support and involvement to cybersecurity program, Cybersecurity policies, Cybersecurity training and awareness programs, Compliance with cybersecurity Legal and regulatory requirements, Cybersecurity change management, Reward and deterrence measures and Cybersecurity monitoring and audit influenced cybersecurity behaviour of members in their organizations and thus this study identified them as the key human factors influencing

organizational cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya.

Table 4.7; Views on Influence of Human Factors Strategies on Cybersecurity behaviour

	Response		
Statements	No	Yes	Total
Top management support and involvement to cybersecurity program	2.80%	97.20%	100.00%
Cybersecurity policies	2.80%	97.20%	100.00%
Cybersecurity training and awareness programs	2.80%	97.20%	100.00%
Compliance with cybersecurity Legal and regulatory requirements	2.80%	97.20%	100.00%
Cybersecurity change management	0.00%	100.00%	100.00%
Reward and deterrence measures	5.60%	94.40%	100.00%
Cybersecurity monitoring and audit	5.60%	94.40%	100.00%

4.4.2 Ranking the various Human Factors

Further, the respondents rated various influences in ascertaining how they would rank these human factors in influencing cybersecurity behaviour of members in organizations. The data obtained from the questionnaire revealed the following findings regarding human factors in cybersecurity management. Majority ranked top management support and involvement to cybersecurity program, Cybersecurity policies, cybersecurity training and awareness programs as factors with the highest influence on cybersecurity culture. Those cited to have least influenced cybersecurity behaviour in these organizations were Cybersecurity change management and Reward and deterrence measures.

Table 4.8; Various human factors ranking

Ranking	1	2	3	4	5	6	7	
Statements								Mean Score
Top management support and involvement to cybersecurity program	65.30%	23.60%	11.10%	0.00%	0.00%	0.00%	0.00%	1
Cybersecurity policies	30.60%	43.10%	15.30%	1.40%	9.70%	0.00%	0.00%	2
Cybersecurity training and awareness programs	11.10%	26.40%	30.60%	22.20%	1.40%	8.30%	0.00%	3
Compliance with cybersecurity Legal	0.00%	9.70%	20.80%	31.90%	25.00%	6.90%	5.60%	4

and regulatory requirements								
Cybersecurity change management	0.00%	1.40%	9.70%	12.50%	15.30%	30.60%	30.60%	6
Reward and deterrence measures	0.00%	2.80%	0.00%	0.00%	16.70%	23.60%	56.90%	6
Cybersecurity monitoring and audit	5.60%	5.60%	6.90%	16.70%	50.00%	11.10%	4.20%	5

Source: Research Data (2020)

4.4.3 Cybersecurity Practices in Respondents' Organizations

The results in Table 4.9 show how respondents responded to the general information about cybersecurity culture in their organizations.

Table 4.9; Perceptions on Cybersecurity Practices

Statements	No	Yes	Total
Adoption of an effective cybersecurity culture will reduce cybersecurity incidents in our organization	0.00%	100.00%	100.00%
Inadequate top management support and involvement to cybersecurity program hinders adoption of favourable cybersecurity culture in our organization	22.20%	77.80%	100.00%
Lack of clear and consistent ICT/cybersecurity policies has resulted in un-coordinated efforts towards adoption of favourable cybersecurity culture in our organization	8.30%	91.70%	100.00%
Employees receive inadequate education, training and awareness programs on cybersecurity, and this has led to unfavorable cybersecurity culture in our organization	19.40%	80.60%	100.00%
Lack of cybersecurity change management techniques such as user involvement in cybersecurity issues, effective communication with departmental heads and other employees and cybersecurity management teams/champions negatively impacts on adoption of favourable	5.60%	94.40%	100.00%
Reward and deterrence measures in our organization influence adoption of favourable cybersecurity culture	11.10%	88.90%	100.00%
Lack of audit and monitoring activities on cybersecurity has led to unfavorable cybersecurity culture in our organization	18.10%	81.90%	100.00%
Inadequate cybersecurity Laws and regulations in the country impacts negatively on adoption of favourable cybersecurity culture in our organization	4.20%	95.80%	100.00%

Source: Research Data (2020)

These results indicate that most respondents agreed with the outlined statements. This revealed existence of gaps between the desired and the current cybersecurity culture state in most of the SMEs studied. The results are in harmony with the 2018 global cybersecurity report conducted by ISACA/CMMI institute. ISACA/CMMI report had found that only 5%

of the 4, 815 organizations studied, believed that they did not have a gap at all, between their current and desired state of cybersecurity culture.

Respondents were also provided with a five-point scale namely Strongly Agree(SA), Agree(A), Neutral(N), Disagree(D) and Strongly Disagree(SD) from which they were required to select responses that described cybersecurity situations in their respective organizations. The topics of response included Favourable Organizational Cybersecurity culture, Top Management Support and Involvement to cybersecurity program, Cybersecurity Policy, Cybersecurity Change management, Cybersecurity training and awareness programs, Reward and Deterrence measures, Cybersecurity Monitoring and Audit and Compliance with cybersecurity Legal and regulatory requirements.

4.4.4 Cybersecurity Culture in the SMEs studied

The research instrument also intended to establish the level of agreement/disagreement on various statements relating to favourable cybersecurity culture in organisation studied. The findings indicated in table 4.10 shows varied responses from one organisation to another.

Table 4.10; Descriptive Analysis for Favourable Organizational Cybersecurity culture

Statements	SD	D	N	A	SA	Mean	Std. Dev
There are physical cybersecurity products like cybersecurity technologies (such as biometric and access control system) and visual personnel security (such as staff badges) in our organization	8.3%	20.8%	25.0%	36.1%	9.7%	3.18	1.13
There are audible and visible cybersecurity behaviour patterns such as slogans, ceremonies and symbols in our organization	2.8%	55.6%	15.3%	12.5%	13.9%	2.79	1.15
Cybersecurity confidentiality is a desired cybersecurity value for our organization	2.8%	2.8%	22.2%	19.4%	52.8%	4.17	1.048
Cybersecurity integrity is a desired cybersecurity value for our organization	5.6%	11.1%	5.6%	40.3%	37.5%	3.93	1.179
My employer understands my roles and responsibilities relating to cybersecurity	2.8%	11.1%	12.5%	30.6%	43.1%	4.00	1.126
I view cybersecurity activities in our organization as NOT an overhead activity to my daily work routine	13.9%	18.1%	11.1%	41.7%	15.3%	3.26	1.311
In the organization, there is commitment to the ideal cybersecurity expectations	11.1%	9.7%	15.3%	36.1%	27.8%	3.60	1.296
If you had a cybersecurity threat, are you likely to be aware	19.4%	2.8%	9.7%	44.4%	23.6%	3.50	1.404

I clearly understand my roles and responsibilities relating to cybersecurity	11.1%	11.1%	2.8%	36.1%	38.9%	3.81	1.36
Cybersecurity availability is one of the desired cybersecurity values for our organization	2.8%	16.7%	5.6%	38.9%	36.1%	3.89	1.157
Understanding of topics covered by the ICT/cybersecurity policy such as E-mail, Backup, Password, Virus, malicious code worms, IoT and BYOD	2.8%	20.8%	16.7%	26.4%	33.3%	3.67	1.222
Overall mean score						3.61	

Source: Research Data (2020)

First, the study established whether physical cybersecurity products such as cybersecurity technologies (for example biometric and access control system) and visual personnel security (such as staff badges) have been deployed in organizations studied. The results showed that 36.1% agreed and 9.7% strongly agreed while 20.8% disagreed and 8.3% strongly disagreed. These findings suggest that not all of the studied SMEs had implemented physical cybersecurity products such as biometric and access control system and visual personnel security such as staff badges. The mean of 2.79 indicates that respondents disagreed that there were audible and visible cybersecurity behaviour patterns such as slogans, ceremonies, and symbols in their organizations. The results further showed that respondents agreed that cybersecurity confidentiality, cybersecurity integrity and cybersecurity availability were a desired cybersecurity value in their workplace. The study also enquired whether respondents view cybersecurity activities in their organization as NOT an overhead activity to their daily work routine and this had a mean of 3.26 an indication of varying responses from respondents with some agreeing and other disagreeing. The statements on whether respondent is likely to be aware if he/she had cybersecurity threat, whether respondents clearly understood their roles and responsibilities relating to cybersecurity, whether their employer understood own roles and responsibilities concerning cybersecurity and finally on whether the respondents understood cybersecurity policy topics as covered by the ICT/cybersecurity policy had mean score close to 4.0 which implied that most respondents agreed.

Most SMEs studied had put in place several measures to promote favourable cybersecurity culture in their organizations as indicated by an overall mean scoring of 3.61. None the less, these findings indicated some unfavourable cybersecurity culture practices among the studied organizations that demands attention.

4.4.5 Top Management Support and Involvement to Cybersecurity Program

The study further established about top management support and involvement to cybersecurity program in development of favourable cybersecurity culture in SMEs that provide enterprise wide IS solutions. The results showed that support and involvement of top management in cybersecurity programs varied from one organisation to another as indicated by agreement and disagreement with the statements in Table 4.11 below. For instance, on top management commitment of adequate funds 33.3% disagreed and 5.6% strongly disagreed while 25.0% agreed and 12.5% strongly agreed. The finding on cybersecurity funding echoes those noted by Serianu(2017) that most SMEs operates below the cybersecurity poverty line and therefore do not have the minimum level of cybersecurity in place.

Table 4.11; Descriptive Analysis for Top Management Support and Involvement

Statements	SD	D	N	A	SA	Mean	Std Dev
Top management commit adequate funds for cybersecurity activities	5.6%	33.3%	23.6%	25.0%	12.5%	3.06	1.15
Top management gives strong and consistent support towards adoption of favourable cybersecurity practices	11.1%	2.8%	18.1%	47.2%	20.8%	3.64	1.18
Top management regularly receive reporting on the status of cybersecurity status	11.1%	11.1%	20.8%	44.4%	12.5%	3.36	1.18
Overall mean score						3.35	

Source: Research Data (2020)

4.4.6 Cybersecurity Policy

The study further sought to establish cybersecurity policy contribution in adoption of favourable organisational cybersecurity culture among the SMEs that provide enterprise wide IS solutions. There was agreement with most statement on cybersecurity related policies which implied that these organisations had cybersecurity policies in place. However, majority of the respondents were not aware that their ICT policy is regularly revised or updated as indicated by mean response of 2.92.

Table 4.12; Descriptive Analysis for Cybersecurity Policy

Statements	SD	D	N	A	SA	Mean	Std. Deviation
There are documented clear and consistent ICT/cybersecurity policies and guidelines that act as a basis for shared cybersecurity beliefs and values	0.0%	11.1%	15.3%	54.2%	19.4%	3.82	0.877
Employees are aware, understand and accept ICT/Cybersecurity policy rules and guidelines	0.0%	8.3%	13.9%	61.1%	16.7%	3.86	0.793
Users of ICT systems abide by ICT/cybersecurity policies	2.8%	19.4%	18.1%	52.8%	6.9%	3.42	0.975
The ICT policy is regularly revised or updated	11.1%	33.3%	27.8%	8.3%	19.4%	2.92	1.286
Overall Mean score						3.50	

Source: Research Data (2020)

4.4.7 Cybersecurity Change Management

Respondent had diverse opinions with regard to the statement on change management. While majority agreed to these statements as indicated by overall mean response of 3.73 on inadequate change management initiatives in their organization, others disagreed as indicated in Table 4.13. For instance, only a combined 23.60% disagreed and strongly disagreed that there was inadequate mechanism to handle criticism and negative perceptions about cybersecurity.

Table 4.13; Descriptive Analysis for Cybersecurity Change Management

Statements	SD	D	N	A	SA	Mean	Std Dev
Absence of a change management strategy is a hindrance to the adoption of favourable cybersecurity culture in our organization	8.30%	9.70%	13.90%	37.50%	30.60%	3.72	1.24
There is inadequate mechanism to handle criticism and negative perceptions about cybersecurity	0.00%	23.60%	13.90%	34.70%	27.80%	3.67	1.13
Top management provide strong hierarchical structures for effective communication on cybersecurity with departmental heads and other employees	8.30%	5.60%	12.50%	44.40%	29.20%	3.81	1.17
Overall mean score						3.73	

Source: Research Data (2020)

4.4.8 Cybersecurity Training and Awareness Programs

The study established practices on cybersecurity training and awareness programs in promotion of favourable cybersecurity culture. The results in this section indicate that cybersecurity training and awareness programs varied from one organisation to another as in Table 4.14. On whether new employees are given cybersecurity awareness in cybersecurity issues, 34.7% agreed and 13.9% strongly agreed while 22.2% disagreed and 5.6% strongly disagreed. Similarly, on whether employees frequently receive training on cybersecurity that informs them on cybersecurity issues and consequences of cyber abuses, 25.0% agreed and 11.1% strongly agreed while 20.8% disagreed and 6.9% strongly disagreed. The findings implied that there was differential provision of cybersecurity training and awareness programs among SMEs that provide enterprise wide IS solutions.

Table 4.14; Descriptive Analysis for Cybersecurity Training and Awareness Programs

Statements	SD	D	N	A	SA	Mean	Std Dev
New employees are given cybersecurity awareness programme in cybersecurity issues	5.6%	22.2%	23.6%	34.7%	13.9%	3.29	1.13
Employees frequently receive training on cybersecurity that informs them on cybersecurity issues and consequences of cyber abuses	6.9%	20.8%	36.1%	25.0%	11.1%	3.13	1.09
The cybersecurity training programs are customized to individual awareness, technical difficulty or departmental risk profile	15.3%	48.6%	11.1%	18.1%	6.9%	2.53	1.16
Employees in our organization know and understand cybersecurity best practices and their application on real live situation	8.3%	5.6%	8.3%	62.5%	15.3%	3.71	1.07
Overall Mean Score						3.16	

Source: Research Data (2020)

4.4.9 Reward and Deterrence Measures

The findings on reward and deterrence measures revealed that some organisation had instituted rewards and deterrence measures while other had not as indicated by Table 4.15. These finding implied that not all SMEs that provide enterprise wide IS solutions had rewards and deterrence measures in place to promote favourable culture of cybersecurity culture in their workplace.

Table 4.15; Descriptive Analysis for Reward and Deterrence

Statements	SD	D	N	A	SA	Mean	Standard Deviation
Clear procedure in place to punish members who do not abide by ICT/cybersecurity policies and regulations	8.3%	8.3%	22.2%	30.6%	30.6%	3.67	1.23
Our organization acknowledges good cybersecurity behaviour by rewarding security compliant individuals	8.3%	20.8%	30.6%	33.3%	6.9%	3.10	1.08
Our organization strives for ideal cybersecurity achievements and material rewards for success	13.9%	19.4%	16.7%	29.2%	20.8%	3.24	1.36
Overall mean score						3.33	

Source: Research Data (2020)

4.4.10 Cybersecurity Monitoring and Audit

In establishing whether SMEs providing enterprise wide IS solutions conduct cybersecurity monitoring and audit to promote a favourable cybersecurity culture, Table 4.16 show that some organisation had initiated visible cybersecurity monitoring and audit measures while had not. These findings implied that there were differential adoption of cybersecurity monitoring and audit among SMEs that were surveyed.

Table 4.16; Descriptive Analysis for Cybersecurity Monitoring and Audit

Statements	SD	D	N	A	SA	Mean	Std Dev
My organization routinely conduct cybersecurity audit and maintain data of cybersecurity vulnerability and intrusion attempts	6.9%	33.3%	23.6%	27.8%	8.3%	2.97	1.11
There is mechanism to ensure effective monitoring of cybersecurity systems	8.3%	5.6%	18.1%	54.2%	13.9%	3.60	1.07
There is mechanism in place to ensure effective monitoring of user violation of ICT/cybersecurity policies	2.8%	11.1%	19.4%	43.1%	23.6%	3.74	1.03
The management is responsive towards monitoring and control comments	13.9%	9.7%	16.7%	52.8%	6.9%	3.29	1.18
Overall mean score						3.40	

Source: Research Data (2020)

4.4.11 Compliance with cybersecurity Legal and regulatory requirements

Compliance with cybersecurity Legal and regulatory requirements was the final factors that study sought to find out about. The results show that respondent had diverse opinions as

indicated by those who disagreed and those who agreed. Table 4.17 shows that in some organisation there was compliance with cybersecurity Legal and regulatory requirements while in other there was opinion that compliance to cybersecurity regulations and practices was not adhered to.

Table 4.17; Descriptive Analysis for Compliance with cybersecurity Legal and regulatory requirements

	SD	D	N	A	SA	Mean	Std. Deviation
There are not enough Government and industry regulations to ensure that personal information is protected from loss, misuse, unauthorized access or disclosure	13.9%	31.9%	15.3%	22.2%	16.7%	2.96	1.337
Employee in our organization signs information security non-disclosure agreement during each new employee on boarding process	15.3%	2.8%	8.3%	40.3%	33.3%	3.74	1.363
Cybersecurity regulations and practices are adhered to in our organization	15.3%	5.6%	13.9%	47.2%	18.1%	3.47	1.289
Overall mean score						**3.39**	

Source: Research Data (2020)

4.5 Inferential Statistics

Pearson correlation analysis and multiple regression analysis consisted the inferential statistics conducted by this study.

4.5.1 Correlation Analysis

To establish the relationship between the study variables, correlation analysis was done. Pearson correlation coefficient was used as it is more appropriate for interval data such as the mean of the Likert scale items from the questionnaire (Sekaran & Bougie,2013). Correlation between various human factors and favourable cybersecurity culture was calculated and presented as in Table 4.18.

The result findings show that favourable cybersecurity culture is positively correlated to all the independent variables (the human factors). The positively correlated human factors imply that when any of the human factors goes up, favourable cybersecurity culture also goes up and when any of the human factors goes down, the favourable cybersecurity culture goes down too.

Table 4.18; Correlation Matrix

		X_1	X_2	X_3	X_4	X_5	X_6	X_7	Y
Top Mgmt. Support (X_1)	r	1							
Cyber security policy (X_2)	r	-.098	1						
Change management (X_3)	r	.051	-.013	1					
cyber security training and awareness (X_4)	r	.095	.095	-.146	1				
Reward and Deterrence (X_5)	r	-.055	.232*	.512**	.262*	1			
Monitoring and Audit (X_6)	r	-.066	.515**	.135	.329**	.650**	1		
legal and regulations compliance (X_7)	r	-.028	.040	.146	.256*	.258*	.152	1	
Favourable organizational Cybersecurity culture	r	.433**	.264*	.330**	.267*	.514**	.464**	.135	1
	Sig. (2-tailed)	0.000	0.025	0.005	0.023	0.000	0.000	0.258	
	N	72	72	72	72	72	72	72	72

**** Correlation is significant at the 0.01 level (2-tailed).**
*** Correlation is significant at the 0.05 level (2-tailed).**

Source: Research Data (2020)

The correlation matrix above indicates the correlation coefficients and p-values between the study variables. The results show that top management support and involvement and organisational cybersecurity culture had a correlation of r=0.433 (p=0.000) and implies that top management support and involvement is positively and significantly associated with favourable organisational cybersecurity culture. The finding suggests that enhancing top management support and involvement will result to positive change in organisational cybersecurity culture.

The results also show that cybersecurity policy and favourable organisational cybersecurity culture had a correlation of r=0.264 (p=0.025). This implies that cybersecurity policy is positively and significantly associated with favourable organisational cybersecurity culture. The finding implied that increasing cybersecurity policy will result to positive increase in organisational cybersecurity culture.

The correlation between cybersecurity change management and organisational cybersecurity culture was r=0.330 (p=0.005) which indicated that cybersecurity change management is positively and significantly associated with favourable organisational cybersecurity culture. These findings implied that increasing cybersecurity change

management will result to positive increase in favourable organisational cybersecurity culture.

The correlation between cybersecurity training and awareness and favourable organisational cybersecurity culture was r=0.267 (p=0.023) which also indicated that cybersecurity training and awareness is positively and significantly association with favourable organisational cybersecurity culture.

The results showed that reward and deterrence had a correlation of r=0.514 (p=0.000), implying positive and significant association with organisational cybersecurity culture. Monitoring and audit had a correlation of r=0.464 (p=0.000) and this implied that Monitoring and audit is positively and significantly associated with favourable organisational cybersecurity culture. The finding implied that enhancing Monitoring and audit will result to positive increase in favourable organisational cybersecurity culture.

Legal and regulations compliance (r=0.135, p=0.258) had positive and not significant association with favourable organisational cybersecurity culture. These finding implied that increasing legal and regulations compliance would not necessarily lead to favourable cybersecurity culture among the SMEs that provide enterprise wide IS solutions in Kenya. Table 4.19 below is the summary of correlation interpretations.

Table 4.19; Summary of the interpretation of Correlation Output

Independent Variable	**The dependent variable**	**Correlation value(r)**	**Direction**	**Significance**
Top management support and involvement	Favourable cybersecurity culture	.433	Positive	0.000 Very strong significance
Cybersecurity policy		.264	Positive	0.025 strong significance
Cybersecurity change management		.330	Positive	0.005 strong significance
Cybersecurity training and awareness programs		.267	Positive	0.023 strong significance
Reward and deterrence		.514	Positive	0.000 very strong significance

Cybersecurity monitoring and audit		.464	Positive	0.000 very strong significance
Compliance with cybersecurity legal and regulatory requirements		.135	Positive	0.258 no significance

4.5.2 Regression Analysis

The relative role of each human factor as well as the joint effect of all the human factors on favourable cybersecurity culture was determined through multiple regression analysis. This was used to establish how the key human factors collectively affect favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya. The model summary of the multiple linear regression on the key human factors and favourable cybersecurity culture is illustrated in Table 4.20.

The model summary indicates that all human factors (independent variables) jointly accounted for 54.4% (R-square=.544) of variation in favourable cybersecurity culture (dependent variable). 45.6% of variation in favourable cybersecurity culture was unexplained for and this is covered by factors not considered by this research.

Table 4.20; Model Summary

Model	R	R-Square	Adjusted R-Square	Std. Error of the Estimate
1	.737[a]	.544	.494	.49231

a. Predictors: (Constant), Legal and regulations compliance, Top Mgmt. Support, change management, Reward and Deterrence, cybersecurity training and awareness, Cybersecurity policy, Monitoring and Audit

Source: Research Data (2020)

ANOVA results on other hand show that F-statistics = 10.887 with a corresponding p-value =0.000. These findings show that model used to predict the effect of human factors on favourable cybersecurity culture among SMEs providing enterprise wide IS solutions was statistically significant. The model had a good fitness hence suitable to predict the effect of top management support and involvement, cybersecurity monitoring and audit, cybersecurity policy, reward and deterrence measures, cybersecurity change management,

cybersecurity training and awareness programs and compliance with cybersecurity legal and regulatory requirements on cybersecurity culture among SMEs providing enterprise wide IS solutions.

Table 4.21; ANOVA Results

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	18.471	7	2.639	10.887	.000b
	Residual	15.512	64	0.242		
	Total	33.982	71			

a Dependent Variable: Favourable Cybersecurity culture
a. Predictors: (Constant), Legal and regulations compliance, Top Mgmt. support, Change management, Reward and Deterrence measures, Cybersecurity training and awareness, Cybersecurity policy, Monitoring and Audit

Source: Research Data (2020)

The results indicated in Table 4.22 show the regression coefficients of the regression model that was used to predict the effect of human factors on cybersecurity culture among SMEs providing enterprise wide IS solutions. Regression coefficients are represented by β values.

Table 4.22; Regression Coefficients

	β	Std. Error	Beta	t	Sig.
(Constant)	0.771	0.636		1.213	0.230
Top Management Support and Involvement	0.438	0.083	0.457	5.298	0.000
Cybersecurity Policy	0.183	0.131	0.14	1.4	0.166
Cybersecurity Change management	0.147	0.104	0.154	1.41	0.163
Cybersecurity training and awareness programs	0.095	0.094	0.099	1.015	0.314
Reward and Deterrence	0.249	0.123	0.284	2.023	0.047
Cybersecurity Monitoring and Audit	0.182	0.132	0.185	1.381	0.172
Compliance with cybersecurity Legal and regulatory requirements	-0.005	0.063	-0.007	-0.08	0.936

a Dependent Variable: Favourable Cybersecurity culture

Source: Research Data (2020)

Optimal Model

$Y = \mathbf{0.771} + \mathbf{0.430}X_1 + \mathbf{0.183}X_2 + \mathbf{0.147}X_3 + \mathbf{0.095}X_4 + \mathbf{0.249}X_5 + \mathbf{0.182}X_6 - \mathbf{0.005}X_7 + \varepsilon$

Y=organizational Cybersecurity culture

X_1 =Top Management Support and Involvement

X_2 =Cybersecurity Policy

X_3 =Cybersecurity Change management

X_4 =Cybersecurity training and awareness programs

X_5 =Reward and Deterrence

X_6 =Cybersecurity Monitoring and Audit

X_7 =Compliance with cybersecurity Legal and regulatory requirements

ε =Error term

4.6 Discussion of the Findings

4.6.1 Effect of the Key Human Factors on Favourable Cybersecurity Culture

Findings from section 4.4.1 above identified Top management support and involvement to cybersecurity program, Cybersecurity policies, Cybersecurity training and awareness programs, Compliance with cybersecurity Legal and regulatory requirements, Cybersecurity change management, Reward and deterrence measures and Cybersecurity monitoring and audit are the key human factors influencing favourable cybersecurity culture among the SMEs studied.

The regression analysis results captured in Table 4.22 show that top management support and involvement had a regression coefficient of β=0.438 and p=0.000 implying that top management support and involvement positively and significantly predicted favourable cybersecurity culture. 1 unit positive change in top management support and involvement would lead to an increase of 0.438 units in cybersecurity culture. The results further indicated that cybersecurity policy had a regression coefficient of β=0.183and p=0.166 implying that that cybersecurity policy positively and not significantly predicted favourable information security culture. 1 unit positive change in cybersecurity policy would lead to a positive change of 0.183units in cybersecurity culture. The presented results also show that cybersecurity training and awareness programs had regression coefficient of β=0.095 and p=0.314 implying that cybersecurity training and awareness programs positively and not significantly predicted favourable cybersecurity culture. 1 unit positive change in cybersecurity training and awareness programs would lead to 0.095units increase in cybersecurity culture. Findings relating to top management support and involvement, cybersecurity policy and cybersecurity training and awareness programs are very consistent with findings determined by Martins & Da Veiga(2015) who identified management, policies, awareness and compliance as critical mechanisms contributing to information security positive culture.

Reward and deterrence measures had a regression coefficient of β=0.249 and p=0.047 which implies that reward and deterrence activities positively and significantly predicted

favourable cybersecurity culture. This is in line with Karwowski & Glaspie(2018) argument that reward and deterrence is a key human factors for enhancing and cultivating information security culture in organizations. 1 unit positive change in Reward and deterrence measures would results to increase of 0.249units in cybersecurity culture.

The regression analysis results further show that cybersecurity change management had regression coefficient of β=0.147 and p=0.163 which implies that cybersecurity change management positively and not significantly predicted favourable cybersecurity culture. 1 unit positive change in cybersecurity change management would lead to positive change of 0.147 units in cybersecurity culture. Cybersecurity monitoring and audit had regression coefficient of β=0.182 and p=0.172 which also implies that cybersecurity monitoring and audit positively and not significantly predicted favourable cybersecurity culture. 1 unit positive change in Cybersecurity monitoring and audit would results to increase of 0.182 units in cybersecurity culture. These finding are inline with findings from Alhogail, mirza & barkary (2015).

The study did not find any statistical support for compliance to Legal and regulatory requirements. Compliance with cybersecurity Legal and regulatory requirements had regression coefficient of β= -0.005 and p=0.936 implying that compliance with cybersecurity Legal and regulatory requirements negatively and not significantly predicted favourable cybersecurity culture. A unit increase in compliance with cybersecurity Legal and regulatory requirements would lead to decrease of 0.005 units in cybersecurity culture. Result findings on compliance with cybersecurity Legal and regulatory requirements are contrary to those of Alhogail, mirza & barkary (2015) that standards and regulations are important human factor to employees' security behaviour in organizations and this may be explained by lack of effective enforcement of legal and regulatory requirements as argued by Serianu(2014) and also the non-adoption of standard security frameworks by Kenyan SMEs.

From the foregoing discussion, all except one of the hypotheses tested were in line with previous research work. Table 4.23 below summarizes the results of hypotheses testing.

Table 4.23; Summary of Hypothesis Testing

Relationship	Hypothesis	Result
Top Management Support and Involvement	H1	Supported
Cybersecurity Policy	H2	Supported

Cybersecurity training and awareness programs	H3	Supported
Compliance with cybersecurity Legal and regulatory requirements	H4	Not Supported
Cybersecurity Change management	H5	Supported
Reward and Deterrence measures	H6	Supported
Cybersecurity Monitoring audit	H7	Supported

4.6.2 Appropriate Roadmap that can be used to Enhance Cybersecurity Culture

Arising from the foregoing discussion on regression analysis, apart from compliance with cybersecurity Legal and regulatory requirements human factor, all the other human factors positively predicted favourable cybersecurity culture in SMEs providing enterprise wide IS solutions in Nairobi city county. This means that there would be some positive change in favourable cybersecurity culture for every unit increase in these human factors. However, except for the Top Management Support and Involvement together with reward and deterrence measure human factors, which had a statistically significant prediction, the increases were not statistically significant since the p-values are greater than 0.05. This could be attributed to random chance. Those findings can therefore be interpreted for a weak positive effect of Cybersecurity Policy, Cybersecurity Change management, Cybersecurity training and awareness programs and Cybersecurity Monitoring audit on favourable cybersecurity culture among the organizations studied. The research established a weak negative impact between compliance with cybersecurity Legal and regulatory requirements and favourable cybersecurity culture and as such compliance with cybersecurity Legal and regulatory requirements do not positively predict the favourable cybersecurity culture as had been hypothesized.

Figure 4.1 below is an illustration of the constructed model using the regression analysis results findings. Subsequently, the model together with the descriptive analysis results findings were used to come up with an appropriate roadmap that can be used to enhance cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya. The identified roadmap is illustrated by Figure 4.2. Similar to road maps that clearly show direction, the roadmap developed from this study can be used by cybersecurity practitioners to benchmark cybersecurity practices and processes in their effort to promote favourable cybersecurity culture in organizations.

Figure 4.1; Model for Enhancing Cybersecurity Culture in SMEs providing Enterprise wide IS solutions in Nairobi city county in Kenya

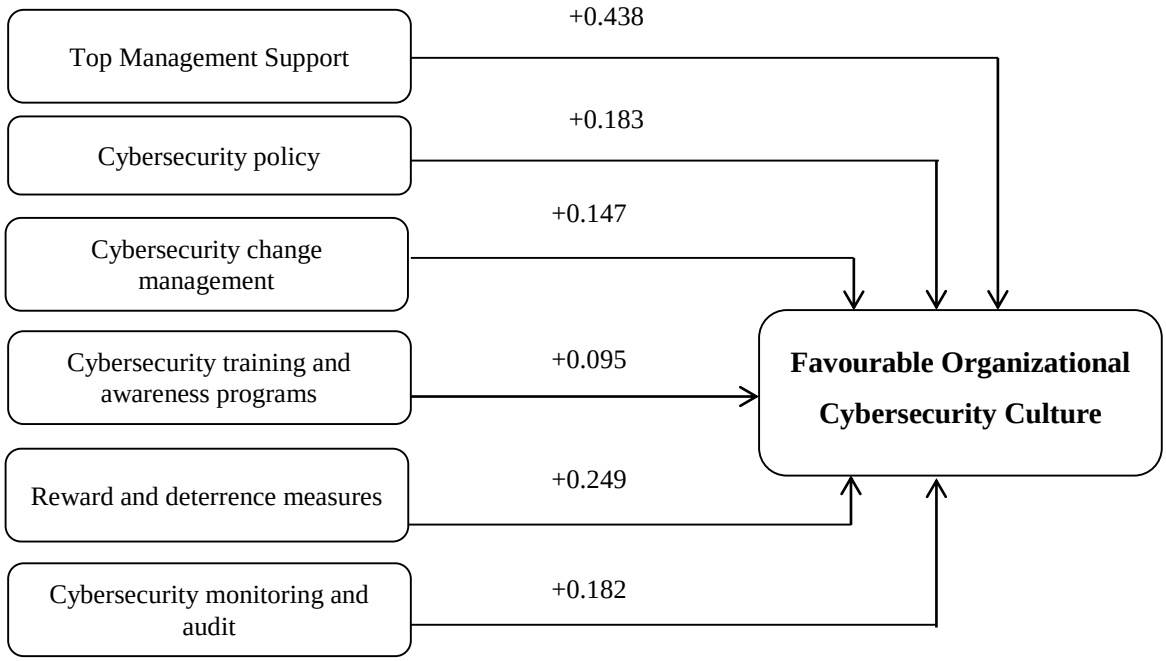
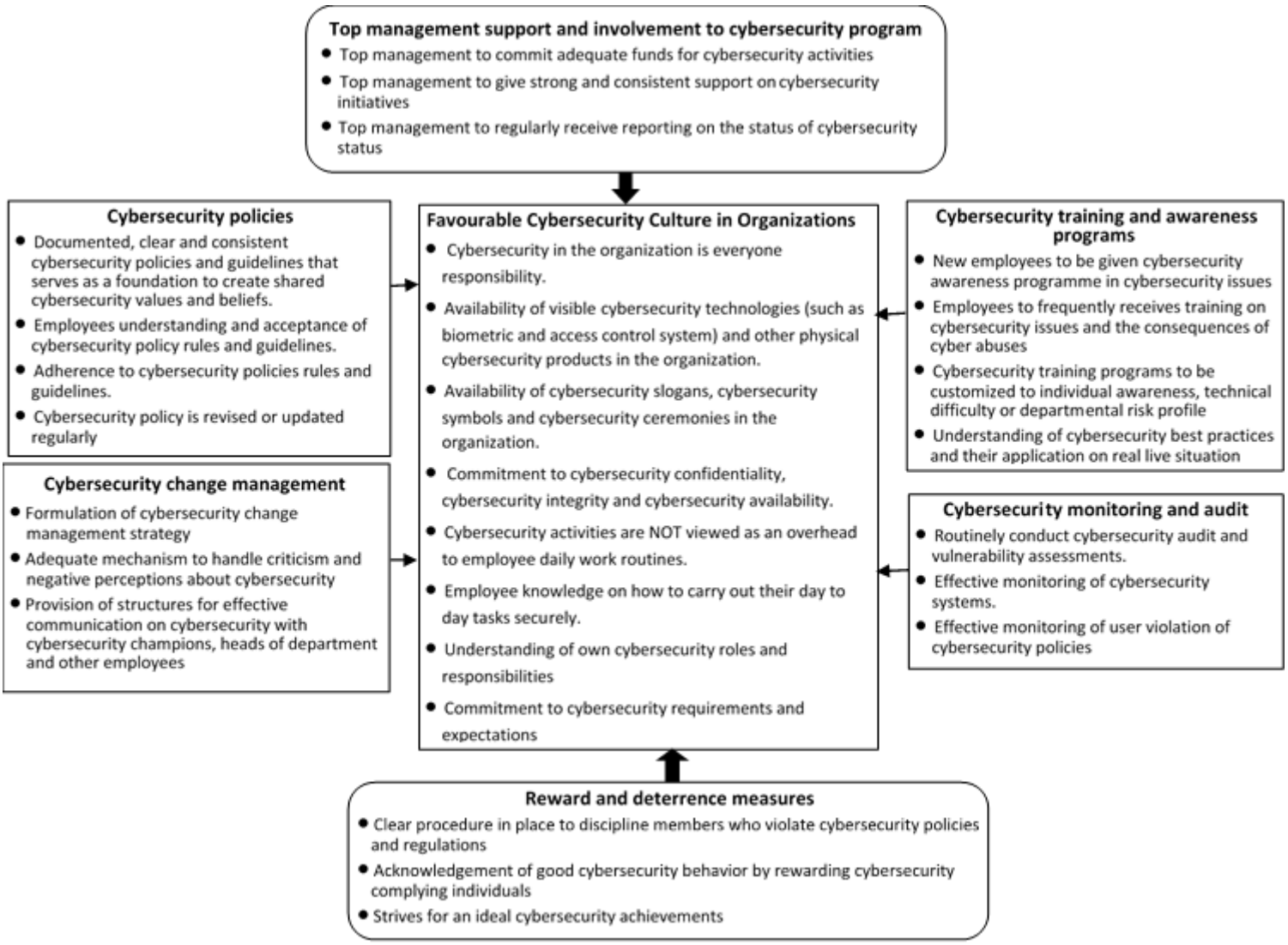


Figure 4.2; A Roadmap for Enhancing Cybersecurity Culture in SMEs providing Enterprise wide IS solutions in Nairobi city county in Kenya



CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The subheadings covered in this chapter include: Summary of the findings, Conclusion and recommendation of this study. The summary of key research findings is presented in consideration of specific objectives and their corresponding research questions thereby demonstrating how the study answered the research questions. The conclusion and recommendation were based on the study findings.

5.2 Summary of Findings

The first objective purposed to determine the effect of key human factors on favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya. Two research questions were answered in addressing this objective: *the key human factors that affect favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya* and *how these key human factors affect favourable cybersecurity culture* among the organizations studied. The first research question was achieved through administration of questionnaires. The generated responses informed of the key human factors that affect cybersecurity culture in SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya. The second research question was answered by inferential analysis on the data generated from the completed questionnaires. Regression analysis findings indicated the effects.

Top Management Support and Involvement, Cybersecurity Policy, Cybersecurity training and awareness programs, Compliance with cybersecurity Legal and regulatory requirements, Cybersecurity Change management, Reward and Deterrence measures and Cybersecurity Monitoring and audit were identified as the Key human factors affecting cybersecurity culture in SMEs providing enterprise wide IS solutions in Nairobi city county in Kenya .With an exception of compliance with cybersecurity legal and regulatory requirements human factor, all the other human factors, that is, top management support and involvement, cybersecurity policy, cybersecurity change management, cybersecurity training and awareness programs, reward and deterrence measures and cybersecurity monitoring and audit were found to be positive predictors of favourable cybersecurity culture in the SMEs studied. A positive change in these human factors would lead to an

increase in favourable cybersecurity culture of the SMEs studied. Detailed findings on how these key human factors affect favourable cybersecurity culture including the human factor on compliance with cybersecurity Legal and regulatory requirements as well as the revised research model were presented in chapter 4 of this document.

The second objective purposed to identify an appropriate roadmap that can enhance cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya. The two research questions generated for this objective entailed: *the human factors strategies that should be developed to enhance the cybersecurity culture* and *how SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya can achieve a favorable cybersecurity culture.* This objective was addressed using the research findings of the multiple regression analysis as well as the issues that arose from descriptive analysis of data. The descriptive analysis of the data collected from our research instrument revealed status of the cybersecurity culture situations within the organizations studied. This in turn informed the developed cybersecurity roadmap. The roadmap was presented as figure 4.2 in chapter 4 of this document.

The regression analysis results indicated that not all positive predictors of the dependent variable (favourable cybersecurity culture) were statistically significant. Only top management support and involvement together with reward and deterrence measures were found to be statistically significant human factors and this suggests their relative importance as critical strategies for instilling favourable cybersecurity culture in organizations providing enterprise wide IS solutions in Nairobi city county. Other human factors strategies that need to be developed among these SMEs are cybersecurity policy, cybersecurity change management, cybersecurity training and awareness programs and cybersecurity monitoring and auditing as they were also found to be positive predictors of favourable cybersecurity culture.

5.3 Conclusion and Recommendation

Previous studies on information security and cybersecurity culture identified Top Management Support and Involvement, Cybersecurity Policy, Cybersecurity training and awareness programs, Compliance with cybersecurity Legal and regulatory requirements, Cybersecurity Change management, Reward and Deterrence measures and Cybersecurity Monitoring and audit as some of the key human factors affecting cybersecurity culture in

organizations. For many organizations, cultivating a favourable cybersecurity culture remains work in progress and that demand an appropriate implementation guidelines and support (ISACA/CMMI, 2018).

The research findings stemming from the descriptive analysis of our research data revealed that a good number of SMEs providing enterprise wide IS solutions in Nairobi city county have put in place several measures to attain favourable cybersecurity culture in their organizations. However, these findings uncovered some unfavourable cybersecurity culture practices in those organizations. Based on the statistical findings of our study, top management support and involvement together with reward and deterrence measures human factors emerged as the significant and positive predictors of favourable cybersecurity culture. Therefore, it can be concluded that cybersecurity practitioners attempting to attain a favourable cybersecurity culture in their organizations need to focus more on developing strategies around these two human factors. Other strategies that need to be developed and implemented are cybersecurity policy, cybersecurity change management, cybersecurity training and awareness programs and cybersecurity monitoring and auditing since they were also found to be positive predictors of favourable cybersecurity culture.

Top management support and involvement ensures among other things that cybersecurity policies, reward and deterrence measures, monitoring and audit, compliance to legal and regulation human factors are addressed in organizations. This study therefore recommends that the top management need to strongly recognise their critical role in promoting a favourable culture of cybersecurity in their organizations.

5.4 Suggestions for Further Research

This research work focused on human factors that impact on favourable cybersecurity culture among SMEs providing enterprise wide IS solutions in Nairobi City County in Kenya. It was established that all the human factors considered by the study accounted for 54.4% of variation in favourable cybersecurity culture. Further study should focus on a wide scope to explain the remaining 45.6% variation in favourable cybersecurity culture. Cybersecurity studies can also be conducted in organizations in different sectors other than ICT and or in different geographical locations.

REFERENCES

Alavi, R., & Islam, S.(2013). Analyzing Human Factors for an Effective Information Security Management System. Research Gate

Alhogail, A., & Mirza, A.(2015). Information Security Culture: A Definition and A Literature Review

Alhogail, A., Mirza, A., & Bakry, S.(2015). A comprehensive Human Factor for Information Security in Organizations. Journal of Theoretical and Applied Information Technology

Al-Kalbani, A.(2017). A Compliance Based Framework for Information Security in E-Government in Oman. Available at: https://www.nascio.org/Publications Accessed on June 18, 2017

Alnatheer, M., Chan, T., & Nelson, K.(2012). A Comprehensive Framework for Cultivating and Assessing Information Security Culture

Areej, A.(2015). Design and validation of information security culture framework. Available at https://www.researchgate.net/publication Accessed on June 18, 2017, 22.

Bandura, A.(2001). Social Cognitive Theory: An Agentic perspective. Retrieved at google scholar on Jan 8, 2020

CBK(2019). Cybersecurity Guideline for Payment Service Providers. Available at https://www.centralbank.go.ke Accessed on December 29, 2019

Da Veiga, A., & Eloof, J.(2010). A framework and assessment instrument for information security culture. Retrieved at google scholar/sciencedirect.com on June 18, 2017

ENISA(2017). Cyber Security Culture in organisations. Available at http://www.enisa.europa.eu Accessed on June 18, 2017

Gupta, M., Sharman, R., & Ada, S.(2009). Theories Used in Information Security Research: Survey and Agenda. Available at https://www.researchgate.net/publication/266645698

Gbedomon, R.(2016). Empowering Women in Technology: Lessons from a Successful Woman Entrepreneur in Kenya Case Study No 10

Godwin, A., & Verdin, D.(2019). Board 51: An Initial Step Towards Measuring First-Generation College Students' Personal Agency: A Scale Validation.

International Energy Agency (2015). Energy Technology Roadmaps a guide to development and implementation.

ISACA(2016).Cybersecurity fundamentals glossary. Accessed at https://www.isaca.org/resources/glossary

ISO Survey(2018). ISO Survey of certifications to management system standards. Accessed at https://www.iso.org/the-iso-survey.html

Kamau, M. (2016). A Framework For Enhancing Compliance In ICT Security Policy: Case Study KPLC

Karwowski, W., & Glaspie, W.(2018). Human Factors in Information Security Culture: A Literature Review

Kimwele et. al (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (1) : 2011

Kiveli, D.(2015). A framework for enforcing the national ICT policy in Kenya Government

Lessa, L., Gebrasilase, T.(2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital

Martins, N., & Da Veiga, A.(2015). An Information Security Culture Model Validated with Structural Equation Modelling. Accessed on June 18, 2017

Martins, N., & Da Veiga, A.(2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Accessed at https://www.sciencedirect.com

Martins, N., & Da Veiga, A.(2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security (2017) 70, pages 72-94

Mohamed, S.(2016). An information security cultural framework: A case study for the Netherlands. Available at: https://scholar.google.com Accessed on December 26, 2019

Mugenda, O., & Mugenda, A.(2003). *Research Methods. Acts Press, Nairobi*

Owens, T., & Onwubiko, C.(2011). Situational Awareness in Computer Network Defense: Principles, Methods and Applications. Available at: https://books.google.co.ke/ Accessed on June 18, 2017

Petrič, G., & Roer, K. (2018). To measure security culture: A scientific approach. Available at: https://hubs.ly/H09Zhtb0 Accessed on January 6, 2020

Laycock, A. & Petric, G. & Roer, K.(2019). The seven dimensions of security culture. Available at: https://get.clt.re/research Accessed on December 11, 2019

Raeside, R., Hall, H., & Middleton, L.(2018). Applications and applicability of Social Cognitive Theory in Information Science Research. Available at https://www.researchgate.net/publication Accessed on February 17, 2020

Rana P., & Dwivedi, K.(2015). Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT). Retrieved at google scholar on June 18, 2017

Rasha, G., & Othman, O.(2016). E-Government- an Information Security Perspective. Available at: https://www.nascio.org/Publications Accessed on June 18, 2017

Sekaran, U., & Bougie, R. (2013). Research Methods for Business - A Skill Building Approach (Vol. 5). Chichester: John Wiley & Sons.

Serianu Ltd et al. (2016). Kenya Cyber Security. Available at: http://serianu.com/downloads/ Accessed on June 18, 2017

Serianu Ltd et al. (2017). Kenya Cyber Security. Available at: http://serianu.com/downloads/Accessed on June 18, 2017

Sherif,E., & Furnell, S., & Clarke, N.(2015). An Identification of Variables Influencing the Establishment of Information Security Culture

Singh, K.(2006). Fundamentals of RESEARCH METHODOLOGY and STATISTICS. Retrieved at https://www.academia.edu/. on June 18, 2017

The ISO Survey(2018). Available at: http://www.iso.org/ the-iso-survey.html. Accessed on June 18, 2017

The Kenya data protection Act 2019. Available at http://kenyalaw.org. Accessed on 2nd February 2020

Tolah, A., Furnell, I & Papadaki, M,(2017). A Comprehensive Framework for Cultivating and Assessing Information Security Culture. *Proceedings of the Eleventh International Symposium on* Human *Aspects of Information Security & Assurance (HAISA 2017)*

UNDP(2015). MSMEs as suppliers to Extractives Industry. Available at www. Undp.org. Accessed on June 18, 2017

Van Niekerk, J., & Von Solms, R.(2006). "Understanding information security culture: A conceptual framework," in Information Security South Africa (ISSA), Johannesburg, South Africa, 2006, pp. 1–10.

Verizon(2017) Data breach investigation report 10th edition. Available at www.ictsecuritymargazine.com Accessed on June 18, 2017

Xu, L.(2016). Building Situational Applications for Virtual Enterprises. Available at: https://scholar.google.com/Accessed on December 26, 2019

Zainudin, D.(2017). Improving Government IT Services Security Using Leadership by Example

APPENDICES

APPENDIX I: COVER LETTER

Dear respondent

RE: VOLUNTARY INVOLVEMENT IN ACADEMIC RESEARCH SURVEY

I am a post graduate student conducting a study on **"Human Factors Affecting Favourable Cybersecurity Culture: A Case of SMEs Providing Enterprise Wide Information Systems (IS) Solutions in Nairobi City County in Kenya"**. This survey aims to seek opinions and perceptions of various individuals in selected SMEs regarding cybersecurity culture. The survey should only take 5-10 minutes of your time.

Your participation in this academic research is highly appreciated. I take this opportunity to reassure you that information provided will be used exclusively for the intended research purpose and that confidentiality of information given will be earnestly safeguarded.

George Njoroge
school of computing and informatics
University of Nairobi,

APPENDIX II: QUESTIONNAIRE SURVEY

INSTRUCTIONS

All questions contained in this questionnaire are part of a survey on Human Factors Affecting Favourable Cybersecurity Culture: A case of SMEs providing Enterprise wide Information Systems Solutions in Nairobi City County in Kenya. In most cases, kindly use the provided response area(s)

SECTION A: INFORMATION ABOUT THE RESPONDENT

1. What is your gender?
   i. Female ( )
   ii. Male ( )

2. Which of these age groups (Years) are you in?
   i. 18 to 25 ( )
   ii. 26 to 35 ( )
   iii. 36 to 45 ( )
   iv. 46 and above ( )

3. What is your highest educational level?
   i. Secondary school or equivalent ( )
   ii. Diploma ( )
   iii. Undergraduate degree ( )
   iv. Postgraduate degree ( )

4. To which hierarchical level does your job description in your organization fit in?
   i. Senior personnel responsible for cybersecurity matters ( )
   ii. ICT head department ( )
   iii. Technical ICT staff ( )
   iv. General user of ICTs ( )

5. How many years have you worked with your organization?
   i. 0 to 1 ( )
   ii. 2 to 3 ( )
   iii. 4 to 5 ( )
   iv. above 5 years ( )

6. (a)Do you think cybersecurity behaviour of individuals in your company has been influenced by the following strategies?

	Initiative	**Yes**	**No**
1	Top management support and involvement to cybersecurity program		
2	Cybersecurity policies		
3	Cybersecurity training and awareness programs		
4	Compliance with cybersecurity Legal and regulatory requirements		
5	Cybersecurity change management		
6	Reward and deterrence measures		
7	Cybersecurity monitoring and audit		
8	Others…….		

(b)Kindly rank the following influences (human factors) on cybersecurity culture in your organization?

	Initiative	**Ranking**
1	Top management support and involvement to cybersecurity program	
2	Cybersecurity policies	
3	Cybersecurity training and awareness programs	
4	Compliance with cybersecurity Legal and regulatory requirements	
5	Cybersecurity change management	
6	Reward and deterrence measures	
7	Cybersecurity monitoring and audit	

Section B: General Cybersecurity Culture Questions

7. Please indicate with an X to provide your response to below statements.

No	**General Information About Cybersecurity Culture**	**Yes**	**No**
1	Adoption of an effective cybersecurity culture will reduce cybersecurity incidents in our organization.		
2	Inadequate top management support and involvement to cybersecurity program hinders adoption of favourable cybersecurity culture in our organization.		
3	Lack of clear and consistent ICT/cybersecurity policies has resulted in un-coordinated efforts towards adoption of favourable cybersecurity culture in our organization.		
4	Employees receive inadequate education, training, and awareness programs on cybersecurity, and this has led to unfavourable cybersecurity culture in our organization.		
5	Lack of cybersecurity change management techniques such as user involvement in cybersecurity issues, effective communication with departmental heads and other employees and cybersecurity management teams/champions negatively impacts on adoption of favourable cybersecurity culture in our organization.		
6	Reward and deterrence measures in our organization influence adoption of favourable cybersecurity culture.		
7	Lack of audit and monitoring activities on cybersecurity has led to unfavourable cybersecurity culture in our organization.		
8	Inadequate cybersecurity Laws and regulations in the country impacts negatively on adoption of favourable cybersecurity culture in our organization.		

SECTION C: Roadmap for Realizing Favourable Cybersecurity Culture among SMEs Providing Enterprise wide IS Solutions in Nairobi City County in Kenya.

8. Kindly provide your response by checking inside the box most applicable to you or your organization.

No	Favourable Organizational Cybersecurity culture	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	There are physical cybersecurity products like cybersecurity technologies (such as biometric and access control system) and visual personnel security (such as staff badges) in our organization.					
2	There are audible and visible cybersecurity behaviour pattens such as slogans, ceremonies and symbols in our organization.					
3	Cybersecurity confidentiality is a desired cybersecurity value for our organization.					
4	Cybersecurity integrity is a desired cybersecurity value for our organization.					
5	Cybersecurity availability is one of the desired cybersecurity values for our organization.					
6	I view cybersecurity activities in our organization as NOT an overhead activity to my daily work routine.					
7	In the organization, there is commitment to the ideal cybersecurity expectations.					
8	If you had a cybersecurity threat, are you likely to be aware.					
9	I clearly understand my roles & responsibilities relating to cybersecurity.					
10	My employer understands my roles & responsibilities relating to cybersecurity.					
11	I understand the following policy topics as covered by the ICT/cybersecurity policy? i) Password ii) E-mail iii) Virus, worms or malicious code iv) Backup iii) BYOD iv) IoT					
	Top Management Support and Involvement to cybersecurity program	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Top management commit adequate funds for cybersecurity activities					

2	Top management gives strong and consistent support towards adoption of favourable cybersecurity practices					
3	Top management regularly receive reporting on the status of cybersecurity status.					
	Cyber**security Policies**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	There are documented ICT/cybersecurity policies and guidelines that serves as a basis to inform shared cybersecurity and beliefs values.					
2	Employees are aware, understand and accept ICT/Cybersecurity policy rules and guidelines.					
3	Users of ICT systems abide by ICT/cybersecurity policies.					
4	The ICT policy is regularly revised or updated.					
	Cybersecurity Change management	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Absence of a change management strategy is a hindrance to the adoption of favourable cybersecurity culture in our organization					
2	There is inadequate mechanism to handle criticism and negative perceptions about cybersecurity					
3	Top management provide strong hierarchical structures for effective communication on cybersecurity with departmental heads and other employees.					
	Cybersecurity training and awareness programs	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	New employees are offered cybersecurity awareness programme in cybersecurity issues.					
2	Employees frequently receive training on cybersecurity that informs them on cybersecurity issues and consequences of cyber abuses.					
3	The cybersecurity training programs are customized to individual awareness, technical difficulty or departmental risk profile.					
4	Employees in our organization know and understand cybersecurity best practices and their application on real live situation.					

	Reward and Deterrence	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Clear procedures are in place for disciplining members who violate ICT/cybersecurity policies and regulations.					
2	Our organization acknowledges good cybersecurity behaviour by rewarding security compliant individuals.					
3	Our organization strives for ideal cybersecurity achievements and material rewards for success.					
	Cybersecurity Monitoring and Audit	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Our organization routinely conduct cybersecurity audit and maintain data of cybersecurity vulnerability and intrusion attempts.					
2	There is mechanism to ensure effective monitoring of cybersecurity systems.					
3	There is mechanism in place to ensure effective monitoring of user violation of ICT/cybersecurity policies.					
4	The management is responsive towards monitoring and control comments.					
	Compliance with cybersecurity Legal and regulatory requirements	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	There are not enough Government and industry cybersecurity regulations in Kenya					
2	Employee in our organization signs information security non-disclosure agreement during each new employee on boarding process.					
3	Cybersecurity regulations and practices are adhered to in our organization.					

THANK FOR PARTICIPATION