CYBER SECURITY READINESS ASSESSMENT MODEL IN KENYAS' HIGHER LEARNING INSTITUTIONS: A CASE OF UNIVERSITY OF NAIROBI

REUBEN GITAU WAWERU

P54/79726/2015

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENT FOR THE AWARD OF MASTER OF SCIENCE INFORMATION TECHNOLOGY MANAGEMENT, SCHOOL OF COMPUTING AND INFORMATICS,

UNIVERSITY OF NAIROBI

JUNE 2019

DECLARATION

This research project is my original work and has not been presented for a degree in any University.

Signature………………………. Date ………………………

Reuben Gitau

P54/79726/2015

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

Signature……………………. Date ……………………….

Prof. Agnes N. Wausi

School of Computing and Informatics

DEDICATION

To my wife Teresia Wanjiku and the entire family for their support and patience throughout the project cycle.

ACKNOWLEDGMENTS

I wish to convey my sincere appreciation to my Supervisor, Prof. A. Wausi for her immeasurable guidance, encouragement, availability and support during the study. I am also grateful to all my lecturers, staff of School of Computing and Informatics and the entire ICT Centre Directorate-University of Nairobi for the assistance accorded to me in one way or the other.

Thank you All.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS ANC ACRONYMS

BYOD	Bring Your Own Device
C&DC	Communication and Data Centre
CAE	College of Architecture and Engineering
CAVS	College of Agriculture and Veterinary Sciences
CBPS	College of Biological and Physical Sciences
CEES	College of Education and External Studies
CHS	College of Health Sciences
CHSS	College of Humanities and Social Sciences
CIA	Confidentiality Integrity Availability
CIRT	Computer Incidence Response Team
CSR	Cyber Security Readiness
GCI	Global Cybersecurity Index
GTA	Game Theoretic Approach
HHM	Hierarchical Holographic Model
ICT	Information and Communication Technology
ICTC	Information and Communications Technology Centre
IMPACT	International Multilateral Partnership Against Cyber Threat
IS	Information Systems
ITU	International Telecommunications Union
NIS	Network Infrastructure Service
OECD	Organisation for Economic Cooperation and Development

PwC	Price Waterhouse Coopers
R&D	Research and Development
SCADA	Supervisory Control and Data Acquisition
SMIS	Student Management Information Systems
SPSS	Statistical Package for Social Science
UON	University of Nairobi
USS&M	User Support Services and Maintenance

ABSTRACT

Cyber security is an important pillar to effective operations on a network infrastructure integrated with information and communications technology. The world today has rapidly embraced the internet whilst personal, social and professional lives have gone digital. While technology and innovation continue to modernize the way we do things, securing the systems and infrastructure lags behind. Due to the ever evolving and growing advancement in digital crime, the computer and network security becomes a fundamental issue. Information technology networks security objectives seek to maintain confidentiality, integrity and availability. Given the openness and extent of cyberspace, it is possible for offenders to conduct covert attacks and exploit vulnerability in systems. In order to secure the systems, higher learning institutions should conduct extensive direct examination in order to assess the cyber security readiness levels. Research shows that there exist various models which have been developed for cyber security readiness assessment; however, they are customized for developed countries whose cyber networks are much more advanced and may not be directly applicable in the case of developing economies. Therefore, this study developed a suitable model aimed at assessing the cyber security readiness, targeting information communication technology staff form institutes of higher learning in Kenya. In particular, the study investigated the cyber security readiness of ICT personnel from the University of Nairobi with the objective of determine the factors that influence cyber security readiness, develop a model for cybersecurity readiness assessment and conduct a diagnostic assessment of the ICT Staff in regard to their cyber security readiness.

CHAPTER ONE

1 INTRODUCTION

1.1 Background

In the twenty first century, the world has rapidly embraced the internet whilst personal, social business and professional lives interact on cyberspace freely and to a great extent. Cyberspace refers to the electronic world created by interconnected networks of information technology and the information on those networks (Toews, 2010). This includes the entire information substructures that are available through internet, and going beyond boundaries with territories. This ongoing digital revolution has driven unprecedented prosperity and efficiency in the world economy and heavily linked with all aspect of modern life. Governments, public and private intitutions, organizations and business entreprises are moving quickly to adopt modern digital applications and technologies. Resultantly these entities have increasingly become highly reliant on utilization of internet resource for their operations. Gehem, et al. (2015) observes that independencies and the Internet of Things (IoT), where the cyber ecosystems have grown in complexity, the risks involved are much harder to assess, whereas the chances of attacks spreading throughout the system increases.

Zukunft (2015) observes that technological innovations will continue to drive global progress for the foreseable future, and will continue to evolve rapidly. In the wake of this development lie numerous emergent challenges and risks that threaten the cyberspace security and prosperity. Cyber security is the protection of the interests of a person, a society of a nation, inclouding all their information and their non-information based assets that will need protection from the risks that relate to their interaction with the cyberspace (Reid & Niekerk, 2014). PwC (2014) reports that with the increase in number of cyber attacks and data breaches in organisations and institutions, demand from the public for organisations to better protect data integrity confidentiality, and its availability of and that of systems has been on the rise.

Importance of Cyber Security Assessment

Siemens Middle East (2018) observes that security assessments enable organizations to have a clear understanding of the trends in perceptions, practices and poential threats that will affect it’s information system assets. This assessment informs organizations on how to better their data protection initiatives and enhance their security practices. Cyber reasiness is aimed at determining the existing or current levels of cyber security planning, resilience and contigency in place. Cwele (2017) notes that cyber security readiness assesses wether critical organization functions and infrastructure can remain operational with minimal damage in case of a cyber attack. Therefore, there is need for a comprehensive assessment to better understand the status quo of cyber security in an organization.

This study embarked on a cyber security readiness survey, in a process of looking at the current status of cyber readiness in institutions of higher learning. This research evaluates the extent to security readiness by examining human resource capacity, hardware and software infrastructure, the organization of the institutions resources, and day-to-day information and communication technology (ICT) practices within a higher learning institution.

1.2 Problem Definition

Integration of ICTs into the worlds' day-to-day activities is likely to continue; computers and computer networks being indispensable to users' everyday interactions and transactions, computers and internet are increasingly becoming preferred tools that attackers exploit to the detriment of the system owners (Armstrong, et al., 2009). Developing countries face numerous challenges in preventing cyber-attacks against their infrastructure; hardware and software. Existing systems, and to a great extent, technical infrastructure, have a number of vulnerabilities such as the monoculture or homogeneity of operating systems (Gercke, 2012). However, Safianu, et al. (2016) notes that cyber security cannot be described as a technical problem, as the numerous technical advances in information technology have at times failed to produce secure environments.

It is critical for institutions to asses their cyber security readiness aided by a model that suits their unique setup. Higher Learning Institution's ICT section is mandated to provide fundamental security CIA triad: confidentiality (C), integrity (I) and availability (A), for the stored data, redirected through, and processed via its electronic resources. Its ICT ensures efficient and effective use of infrastructure and ICT resources, protection of the resources from attacks, network and system failure, unauthorized access and litigations. In Higher Learning Institutions, ICT base support teaching, learning, research and management of the institution. This study therfore sought to assess cyber security readiness of ICT Staff at the

University of Nairobi, and to comeup with a model that could be used in assessing cyber security readiness and to determin factors influencing cyber security readinesss in Kenyas' Higher Learning Intitutions.

1.3 Objectives of the Study

1.3.1 General Objective

The fundamental aim of the study was to develop a suitable model to use in conducting cyber assessment for security readiness of higher learning institutions in Kenya; thus, to help decision makers to assess cyber security of ICT systems.

1.3.2 Specific Objectives

i. To determine major factors which influence cyber security readiness for Higher Learning Institutions in Kenya

ii. To develop a cyber-security readiness assessment model for Higher Learning Institutions in Kenya

iii. To validate the model for cyber security readiness assessment for Higher Learning Institutions in Kenya.

1.4 Justification

Rahat (2014) observes that higher learning institutions foster forms of technological openness that is not too suited to systems or data in need of strong protection. Also, that the quest for openness, information access and sharing and the bring-your-own-device (BYOD) paradigms is spreading fast in these institutions and are highly depend on IT infrastructure to connect to the network. The growth has affected institutions preparedness for threats and exposed vulnerabilities to which cybercrimes can be perpetrated. Despite cyber threats and risks being unique to each industry, higher education ranks at the top five of the sectors faced with high numbers of cyber-attacks (Kenya Cyber Security Report, 2017). From a data security perspective, these institutions are important due to the fact that they hold immense amounts of data belonging to a huge population. The study by Mello (2018), points out that holding vast amount of data poses a large threat in form of data breach and that a university is more likely to be breached if it is a large university. Findings from this study are aimed to identify the existing weaknesses in campus network and recommend a secure model to address cyber security issues in institutions of higher learning. The researcher believes that findings of this study will eventually lead to deliberate efforts at both management and technical levels to prevent future cyber security breaches.

1.5 Scope

Scope coverage of the research was Information Communication Technology Centre (ICTC) at the University of Nairobi. The Centre has different professionals in various ICT disciplines with clear mandates and specific duties. Of interest to the study was those concern with cyber security matters at the Centre. The Centre is also composed of the staff of interest in the three level (management, project leaders and technical support) of interest to this research within colleges. The findings here can therefore, be inferred to a wider population; extending to other areas would result to replication of data.

1.6 Limitations of the study

The research was focused on Higher Learning Institution’s sections with ICT functions and staff; owing to the fact that not all sections within the colleagues have the technological infrastructure and deployed technical human resource supporting the same.

CHAPTER TWO

2 LITERATURE REVIEW

2.1 Cyber Concepts

Cyberspace poses risks in different forms to an organisation as well as opportunities to be exploited. McClelland (2009) takes note that while technology and innovation has continued to modernize the way we do things, the worldwide community increasingly endures rise in the levels, sophistication and penetration success rates of cybercrimes. The Cyber security challenges and risks are constantly sprouting threats to an organization's ability to attain its objectives and deliver to its core functions. Cybersecurity security includes communication security and computing security (Wang, et al., 2010). This involves managing cyber risks around communication and computing functions of an organization to an acceptable level. Implementation of internet security risk management forms portion of an organization's governance, strategic framework and business continuity throughout the organization.

It is incumbent for organizations to ensure while on the cyberspace they are protecting the availability, integrity, confidentiality and of sensitive customer data, and system to curtail cyber-attacks and data breaches. Assessing cyber security helps in the determination of an organization's readiness to detect, contain, prevent, and respond to the changing cyber or internet threats (PwC, 2014). Cyber security readiness assessment is fundamentally conducted to enable an organization visualize its current security bearing and identify hidden loopholes to be investigated and mitigated. Organisations are encouraged to have periodic assessment of their cyberspace systems security readiness, to monitor progress or any potential deterioration.

2.2 Cyber Security Readiness Assessment

Various studies in readiness assessment have predominantly targeted developed countries and least developed countries in other continents, with greater focus on Information Systems (IS) and eLearning, whilst a few on cyber security. The study done by the International Telecommunication Union ITU (2012) and a team of experts from International Multilateral Partnership Against Cyber Threats (IMPACT), carried out readiness assessment of cyber security on five countries in South Asia categorized in least developed nations. This was aimed at reviewing institutional and regulatory framework, existing critical information infrastructure, and identifying areas of improvement and to recommend establishment of a Computer Incidence Response Team (CIRT). A report by Ryoo, et al., (2009), describes research conducted to assess the level of security readiness of IS for Municipalitien in Rural Pennsylvania. The study, through use of a set of survey instruments, measured three major aspects of a municipality's IS security readiness: infrastructure, literacy and practices.

Locally, a study by Oketch (2014), included a model that developed for eLearning readiness assessment for teaching staff from the Kenyan higher learning institutions. This resercher investigated the e-learning readiness of University of Nairobi lecturers with the main aim of conducting an examiniation and determining which factors influence the eLearning readiness significantly. Another study by Waithaka (2016) sought to find out factors that affect cyber or internet security in public service, specifically Kenyan National Ministries. This researcher's target respondents in the (ICT) Information Communication Technology officers, at the Ministry and the Internal Auditors (IA) tasked in the review of IS.

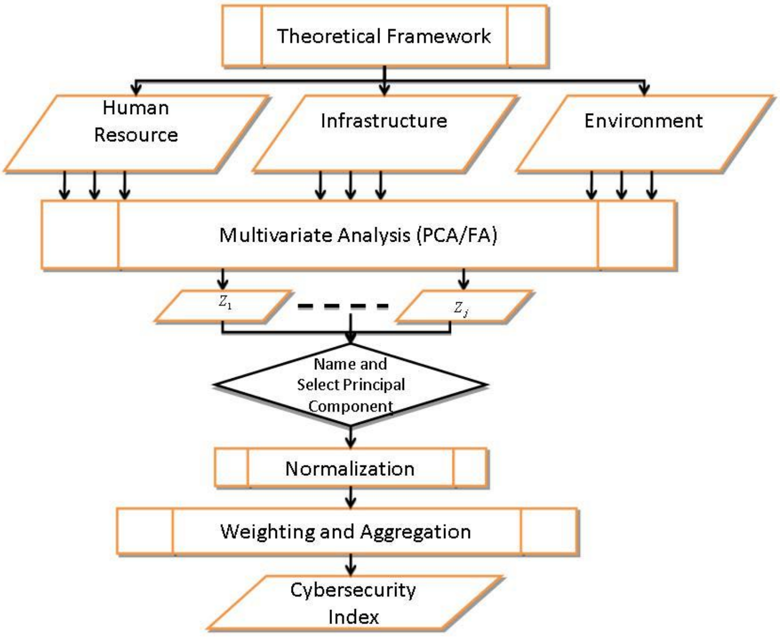
2.2.1 Cyber Security Readiness Assessment Models

Various research and publications on organizational readiness for cyber security provide decision makes with strategies, guidelines, indicators, models and frameworks for assessing their readiness (ITU, 2018; Yunis & Koong, 2015; PwC, 2014; Cheang, 2009). Literature reviewed shows a number of models with varying indicators for cyber security assessment on global, state and institutional levels. The models that have been discussed below include important factors used in public institutions, hence their usefulness in carrying out the research.

2.3.1.1 Cheang (2009) Cyber-Security Readiness Model

A study by Cheang (2009) established a conceptual model used in assessing cyber security readiness of those in public sector for a developing Country, a case of Cambodia. The study prioritized public institution, primarily motivated by the circumstance in which these institutions are documented as highly vulnerable, and targeted in cyber-attacks. The researcher measured the cyber security readiness of in three dimensions: infrastructure, environment, and that of human resource, as shown in the conceptual model Figure 2.1.

Figure 2.1: Cyber-Security Readiness Dimensions



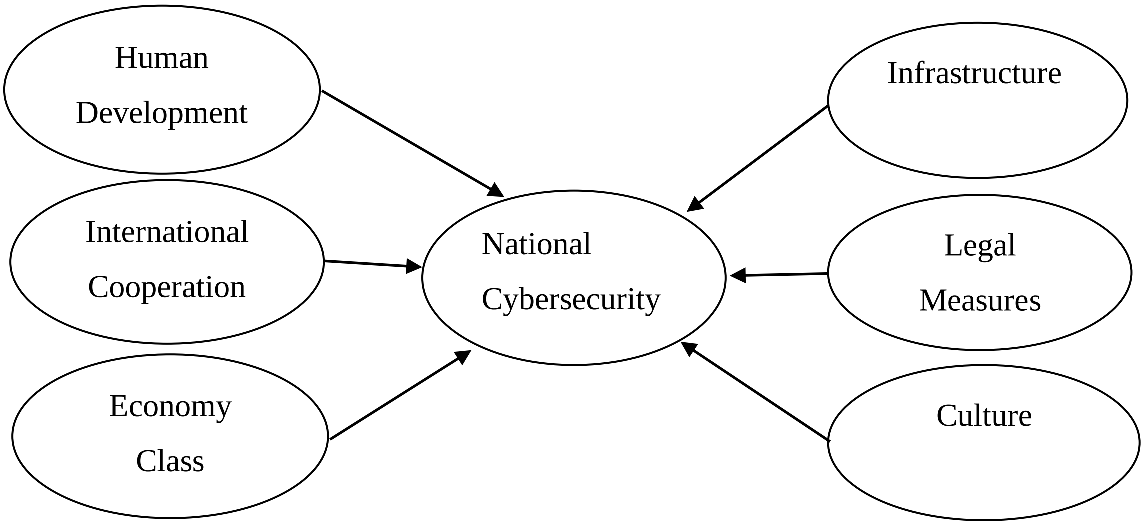
Source: Cheang (2009)

The Human resource dimension has 13 variables, where the 1 to 4 variable measures human capacity in terms of preparedness towards cyber incidents, like having security tools, training of staff and skills of the personnel in IT. Variable 5 to 7 evaluates the capability of IT staff in protecting it's organization against attacks in cyber space. Finally, variable 8 to 10 evaluates the personnel's readiness capability of responding to cyber incidents, and variable 11 to 13 the staff's readiness ability of bounce back from ant cyber incidents experienced. The organization and its resources are categorized into physical substructure to form the infrastructure dimension assessed by variable 14 to 34.

2.3.1.2 Yunis and Koong (2015) Cyber-Security Readiness Model

A proposal by Yunis and Koong (2015) seeks to have an integrated framework for building a cyber-security index, as a necessary tool to compare the performance of nations in terms of initiatives, policies and strategies in cyber security. The study takes into consideration six factors: economic, culture, legal, infrastructure, institutional and human development.

Figure 2.2: Cyber-Security Readiness Factors



Source: Yunis & Kong (2015)

2.3.1.3 ITU (2017) Cyber-Security Readiness Model

ITU (2017) developed a reliable reference model for the purpose of measuring the readiness of nations to cyber security globally, hence raising awareness and different dimensions for cyber matters. One of the ITU's mandate is creation of national CIRT and in particular for developing countries like Kenya and cooperation between like countries. The Global Cybersecurity Index (GCI) model by the ITU therefore assesses each nation's standing in growth or involvement in cyber security. A considerable area of application touch on numerous sectors or industries such as consolidation of roles by ITU in developing self-confidence and also security where ICT is concern. Assessment is rooted on five distinct pillars which are; organizational measures, legal measures, cooperation, capacity building, and technical measures, and then aggregated into an overall score. Essentially, the GCI is a composite indicator which aggregates five individual indicators as summarized in Table1.

Table 2.2.1: Cyber-Security Readiness Indicators Model

Cyber-Security Readiness Indicators	**Explanation of Indicators**
Legal readiness	Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime
Technical readiness	Measured based on the existence of technical institutions and frameworks dealing with cybersecurity
Organizational readiness	Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level
Capacity building readiness	Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
Cooperation readiness	Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Source: ITU (2017)

2.3 Summary of Knowledge gap and Literature Review

This study reviews literature on readiness assessment models in various research work with the view of finding a suitable model for higher learning institutions. Cheang (2009) established a theoretical three-dimension model for assessing readiness of cyber security in public institutions on developing countries. This researcher's model groups ITU (2009) indicators; resources, people, relationships, institutions, policies, budget and procedures, into three dimensions of Environment, Human Resource, and Infrastructure. Yunis and Koong (2005) propose a holistic framework as a tool to compare the performance of countries when considering cyber security initiatives, policies, and strategies. Their model puts into consideration the following factors pertaining to countries: Technological, Legal, Economic, Cultural and International relations.

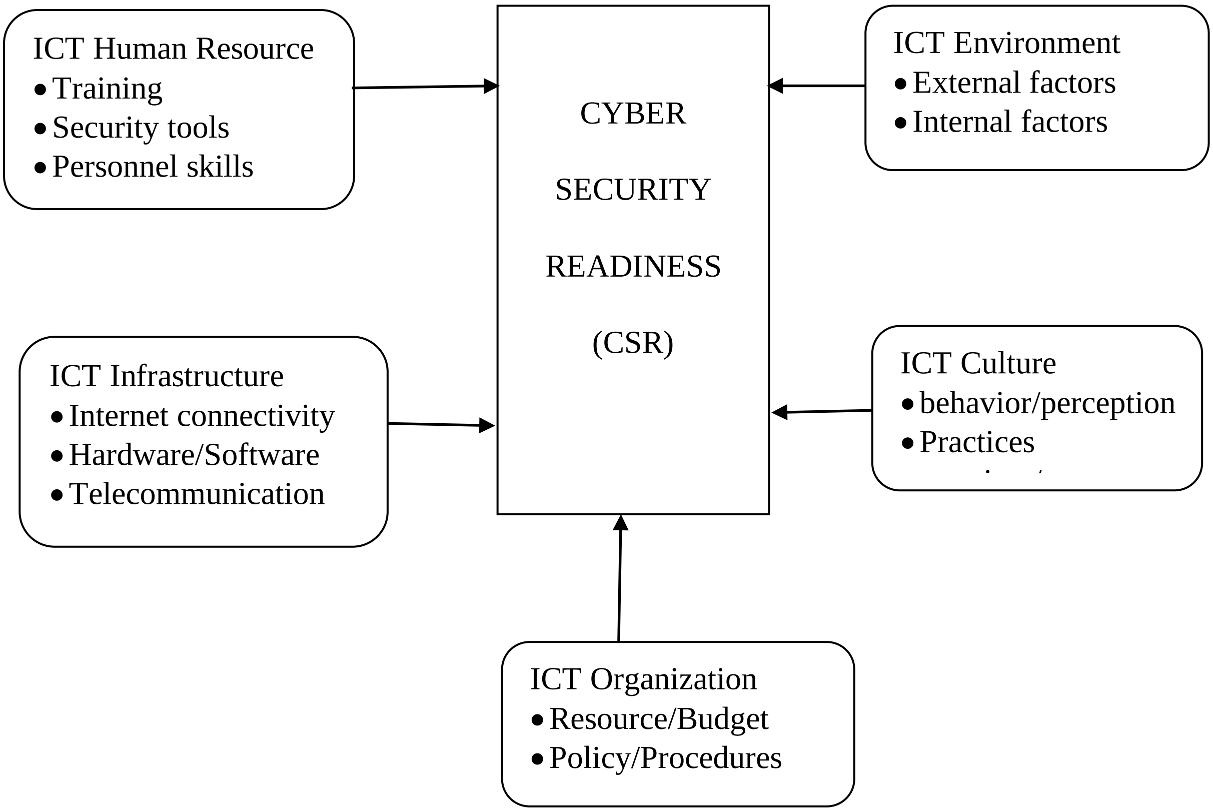
The International Telecommunication Union whose mandate is creation of a national Computer Incidence Response Team (CIRT) and in particular for developing countries (ITU 2017), developed a readiness assessment model for countries globally. Global Cybersecurity Index (GCI) model, assesses countries via a five pillars model including the following indicators: cooperation, legal, technical, capacity building and organizational measures.

2.4 Conceptual Model for Cyber-Security Readiness Assessment

With the following research objectives in mind; (i)determination of factors influencing cyber security readiness in higher learning institutions (ii) developing a suitable model for readiness assessment of higher learning institutions (iii) assessment of cyber security capabilities in higher learning institution, the studies reviewed offer a baseline for this research. From the above literature review, the study proposes composite measures for higher learning institutions in developing economies, which is founded on five dimensions: Human Resource, Infrastructure, Environment, Organization and Culture. The researcher agrees with Cheang (2009) in combining the identified indicators for public organizations into the dimensions of; Environment, Infrastructure and Human Resource, as well as the incorporation of Organizational readiness (ITU 2017) and Culture factor from Yunis and Kong (2015) model.

Indicators were modified as above stated and modeled in recognition of the objective of preparing for, preventing, recovering from and responding to any cyber incidents.

Figure 2.3: Model for Assessing Cyber-Security Readiness



2.4.1 ICT Infrastructure Readiness

ICT Infrastructure is considered as a major cyber security issue that should be used for readiness assessment. This indicator assesses ICT infrastructure facilities such as internet connectivity, telecommunication facilities, bandwidth, broadband access, systems software, and devices.

2.4.2 ICT Human Resource Readiness

The human resource in ICT play a critical role in regard to cybersecurity asset; they conduct the operation such as recovery, preparation, protection, and, responding to cyber incidents. Human resource readiness measures the personnel’s ability in readiness to for cyber incidence and the training tools including technical skill for personnel. The indicator looked into capability of its ICT personnel in protecting the organization, responding and recovering from any kind of cyber incident.

2.4.3 ICT Environment Readiness

The environment indicator discusses external factors and internal factors that affect institution’s ability in tackling cyber incidents that may arise. This assessment is based on factors within and outside the organization like cooperation with third parties, vendors, partners, agencies, legal issues and regulations and authorities.

2.4.4 ICT Culture Readiness

Research suggests that the cultural aspects are very important factors that influence non-compliance behavior by staff. What the staff observe in terms of the daily practice, culture, rituals, and habits in cyber security related matters. It looks at individual perception of various features that make an organization secured from cyber threats This may vary form one institution to another based on differences in norms, values and beliefs across various groups of people.

This indicator evaluates the behavior, perceptions and daily practices of ICT personnel in view of cyber security readiness.

2.4.5 ICT Organization readiness

In order to assess the readiness of an institution’s ICT, it is critical to evaluate policies, procedures, resources and budget allocated for recovering, preventing, and responding to cyber incidences. This indicator evaluates managements abilities and the availability of administrative assets dedicated to cyber security.

CHAPTER THREE

3 RESEARCH METHODS

3.1 Introduction

The chapter lays out the design and methodological approaches for research that was applied in conducting the study. Primarily, the objective of this study was to evaluate cyber security readiness of higher learning institution in Kenya. This chapter therefore outlines the research design to be used for the survey, the method of collecting data, population of the study, and the methods of data analysis applied.

3.2 Research Design

With this study, the researcher intended to assess cyber-security readiness of higher learning institutions in Kenya. To be able to conduct the assessment of higher learning institutions, the researcher found it ideal to do a of case study. This is because a case of study refers to an empirical review that undertakes investigating the subject matter in real-world context, more so when there are no clear boundaries between phenomenon and context (Yin, 2014). The researcher undertook an exporatory using descriptive case of study research design. A descriptive research will involve gathering data corresponding to questions related to present status of the subject under study. Preliminary literature review did not identify academic works that deal with cyber security readiness assessment in the institutions of higher learning.

3.3 Population of Study

Banerjee & Chaudhury (2010) describe population to be the whole group about which some information is needed to be established. Population of the study consisted of ICT personnel from six colleges in University of Nairobi. There are 11 campuses in University of Nairobi hosting various colleges; seven of them located in Nairobi county (the capital city) the rest in other counties. The population comprised entire ICT personnel in the six colleges at the University of Nairobi (UON). All colleges are geographical located within Nairobi in different campuses making it logistically and financially easy to include all of them in the study. The ICT staff are 114 in number, drawn from various specialties and work areas within the University.

Table 3.3.1: General Proportion of ICT Staff

Serial	University of Nairobi Colleges
i.	College of Humanities and Social Sciences (CHSS)
ii.	College of Health Sciences (CHS)
iii.	College of Education and External Studies (CEES)
iv.	College of Biological and Physical Sciences (CBPS)
v.	College of Architecture and Engineering (CAE)
vi.	College of Agriculture and Veterinary Sciences (CAVS)
	Total 114 ICT Staff

Source: University of Nairobi website (2019)

3.3.1 Target Population

Cooper and Schindler (2014) define target population to be people, events, and records that encompass the resercher’s desired-information and can response to measurment question. This study targeted a population of 114 ICT staff in Director’s, Student Management Information Systems (SMIS), User Support Services and Maitenance (USS&M), Network Infrastructure Service (NIS), and Communication and Data Centre (C&DC) sections.

Table 3.3.2: Population of ICT Staff by Section

Section	Number of Staff
Director’s Office	10
Student Management Information Systems (SMIS)	34
User Support Services and Maitenance (USS&M)	29
Network Infrastructure Service (NIS)	11
Communication and Data Centre (C&DC)	30
Total	**114**

Source: Research Data

These sections were in the four strata of intrest to this study (Director, Manager, Project Leader, and Technical) and were working and operadet in the various colleges. Director’s section had 5 members, 3 members in management section, 5 as project leaders and 12 drawn from the technical section.

3.4 Sampling Size and Sample Design

Research sample describes the members of a target population from whom data was collected. A sample examining a percentage of a target population was carefuly selected in order to represent the target population. Kothari (2004) identifies a good sample design as one that results in minor sampling error, one that is feasible in available funds context for research, has better checks and balances for systemic bias, and whose outcome of the sample study can be applied, generally, for the population with a resonable confidence level. In sampling, researcher determines which and how many people,events and records to interview, observe and inspect respectively (Cooper & Schindler, 2014). The resercher selected research design to which the given cost and sample size will have a smaller sampling error.

In this study, purposive sampling technique was applied for the discovery, understanding and gaining insight by selecting a sample from which the can be learned and inform the study. Gay, Mills and Airasian (2012) observe that purposive approach benefits to sampling for case study research is the purposful selection of cases that are rich in information or those from which a great deal of the research problem can be learnt by the researcher.

3.4.1 Sampling Frame

Sampling frame refers to records of all entities from which a representative sample is obtained to be used for the study. Banerjee and Chaudhury (2010) describe a representative sample to be one where all the member of a population having an equivalent, mutually exclusive chance of to be considered for selection. In this study, the sampling frame was the list of directors, managers, project leaders and technical staff of ICTC from the sections in table 3.2. The staff targeted had to be at least 21 years old and at most 60 years old.

3.4.2 Sample Size

Baskarada (2014) argues that in a qualitateive study, it may be difficult or even impossible to obtain a sufficiently large sample for the unit of analysis; in such instances a case study is prefered. A qualitative study focuses on moderately fewer participants, whom charactalisticaly are abile to give a describtion of their experiences and, or what their know with regard to the research phenomenon and questions (Creswell, 2014). When selecting a suitable sample size, Kothari (2004) recommends consideration of two costs: that of data collection and the cost of an incorrect inference that may result in data. Further a researcher must consider the two reasons of wrong nference due to systematic bias or sampling error.

Homogeneous method of sampling was used for the 25 respondents who were purposively selected for a census. Babbie (2010) describes judgmental or purposive sampling as an instance of nonprobality sampling where the people or units of observation are selected based on the researcher's judgment. This applies where the potential respondents will be more representative or most useful. Battaglia (2011) observes that in purposive sampling, given the subjectivity of selection method, it is well suited where small samples are being selected. The samples are mostly from a difinition of restricted a limited geographic coverage, a case where inference to population is not prioritized.

Table 3.4.1: Sample Distribution

Position	**Population**
	N
Directors	5
Managers	3
Project Leaders	5
Technical Staff	12
Total	**25**

3.5 Data Collection Method

The study carried out an online survey through administering online questionnaires with closed-ended questions as an instrument to collect primary data tailored for various indicators in the study. Online survey involves the use of World Wide Web (www) and the internet via e-mail or websites (Babbie, 2010). Potential respondents received an e-mail asking them to go to a web link where the survey resides to fill the closed-ended questions. Jackson (2009), observes that use of closed-ended questions makes it easy for the researcher to analyze statistically whereas open-ended questions are difficult to analyze statistically because data must be coded.

The study used a Likert-type scale (e.g. 1. Strongly disagree, 2. Agree, 3. No Opinion, 4. Agree, 5. Strongly Agree).

The questionnaire consisted of the following sections namely; section A, section B, section C, section D, section E, and section F. To begin with, the first section A, collected demographic data of respondent and college they belong to. Section B of the questionnaire looked at the general cyber security readiness of the individuals. Human resource readiness factor was addressed by questions in Section C that look at training and skills among others. The infrastructure readiness was evaluated in section D listing hardware and software concerns. Section E seeks to evaluate the organization readiness in terms of policies, procedures, budget and resources dedicated to cyber security. Cultural readiness of the staff was evaluated by questions in section F that asks behavior and practices concerns.

3.6 Data Analysis

completeness of the online questionnaires was checked, then a well coded summary was provided. IBM Statistical Package of Social Science (SPSS) Statistic Subscription was utilized as the statistical tool for analying all through. Furthermore, descriptive statistics was put to use in analyzing the data collected and present the outcomes in tabular and charts forms. The summarized data was used to generate frequencies, weighted averages, percentages, and culminative percentages. Staff cyber-security readiness was determined via descriptive statistics, whereas regression analysis conducted determined factors influencing cyber security readiness and to examine suitability of the proposed model to determine their cyber-security readiness. The ITU (2018) assessment model was used in determining the expected level of cyber maturity score. The GCI score was based on a singular outcome through the total score of indicators to measure cyber maturity. This was an assessment that provided an in-depth evaluation of the institutions’ capability to protect its IS resourse in addition to its readiness and efforts against cyber any threats (Hansen, 2016).

CHAPTER FOUR

4 DATA ANALYSIS, FINDINGS AND DISCUSSION

4.1 Introduction

The chapter provides a detailed summary of findings and results therein that were obtained from research done using the CSR survey tool described in depth in Chapter 3. A detailed data analysis obtained in this study is also well documented. The study sought to develop a model that is suitable in the assessment of cyber security readiness at higher learning institutions in Kenya. Specifically, the study looked at human resource, infrastructure, organization, environment and culture readiness. The data was analyzed in accordance with the different levels of study. First, analysis of the characteristics of the sample is presented, followed by results and findings of initial data analysis. Finally, presentation of characteristics, discussion, and analysis of factors in conceptual framework in Chapter 2.

4.2 Preliminary Study

4.2.1 Sample Distribution

The research survey was conducted in the University of Nairobi's ICT Centre directorate in Kenya. Online-administered questionnaires were administered to the 25 staff/heads of Director, Student Management Information Systems, User Support Services and Maitenance, Network Infrastructure Service, and Communivation and Data Centre sections purposively selected for this work.

4.2.2 Response Rate

Fowler (2014) describe response rate as an elementary parameter used in evaluating efforts of collection of data. This refers to number of people that completed the survey devided by the number of those eligible that were sampled, including those who did not respond or were unavailable. The instruments were administered to the selected sections as per the sample size in section 3.4.2. Bernard (2011) observes that there is no limit to the number of respondents constituting a purposive sample provided one obtains the desired information. A census was conducted for the 25 respondents hence 100% response rate in this study.

4.3 Study on ICTC Personnel

A full study was conducted on the sample of 25 members of staff at the ICTC represented in the various section and Twenty-Five responses obtained as per Table

Table 4.3.1: ICTC Staff Sample Response

Stratum	**Sample**	**Response**	**Percentage (%) of Sample Response**
Directors	5	5	100
Managers	3	3	100
Project Leaders	5	5	100
Technical Staff	15	12	100
Total	**25**	**25**	**100**

i. Gender of the Respondents

Census results indicated in the figure 4.1 shows 20 (80%) of the respondents were men whereas the remaining 5 (20%) were women. These results in regard to gender ration may be attributed to domination of men in the technology sector where until recently women had no household names in IT. The findings of Castano (2011) establish that dispite considerable efforts devoted to reaching a gender balance in ICT proffessions, women still make up under 20% of ICT professionals in most Organisation for Economic Cooperation and Development Countries (OECD). Reasons for this disproportion are education; with less than 1 out of 5 computer or engineering bachelors degrees are attained by women. A vicious cycle where fewer women in IT leadership position make the field less attractive to other women or the environment; tech business can be very boisterous and misogynistic (Staiger, 2017). The situation is however changing with time, looking at the younger generations where both boys and girls seem interested and involved in various ICT tools (Tomte, 2011) and the emergence of social media where girls seem to be more involved.

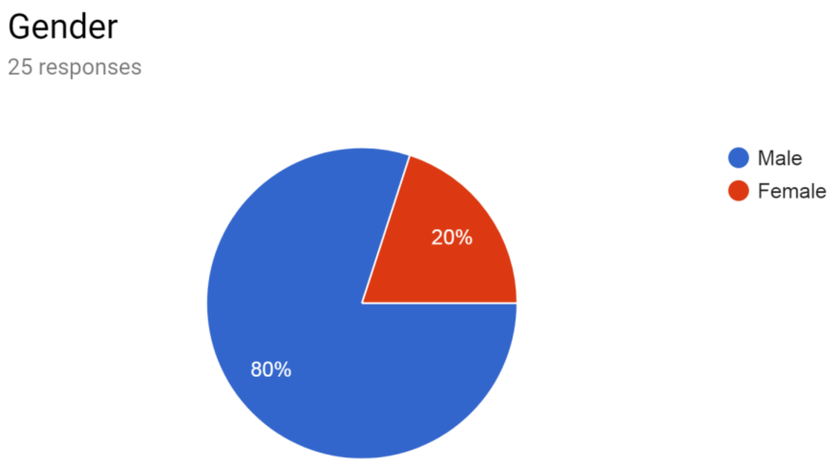


Figure 4.1: Gender of Respondents

ii. Respondents Age Bracket

The findings showed that 56% which is the largest proportion of the ICTC staff respondents to be between ages 31 years and 40 years. Findings tabulated in Table 4.2 show that there was only 4% (1) respondent who was between ages 50 years to 60 years, 24% (6) of the respondents to be between ages 41yeas and 50 years, while the remaining 16% (4) of the respondents to be between ages 21years and 30 years. Accordance to the new NSSF Act, the normal retirment age for public service employees is sixty (60) years of age (Muthaura, et al., 2017).

Table 4.3.2: Respondents Age Bracket

Age Bracket	Frequency	Percent (%)
21-30	4	16
31-40	14	56
41-50	6	24
50-60	1	4
Total	**25**	**100**

iii. Levels of Education

Respondents were asked to state the highest level of education at present and Figure 4.3 shows the outcome. The study revealed that 13 (52%) of the respondents had Master Degree, a further 10 (40%) of the respondents had Bachelor Degree and the remaining 2 (8%) had Diploma. It was observed that none of the respondents selected for the study were either only Certificate holders or attained a Doctorate Degree. This implies that the respondents purposively selected were a good balance of highly skilled and basic level individuals in their area of specialization hence knowledgeable and best candidates in the five areas of the Cyber Security Readiness (CSR) represented in Figure 2.3. The Kenya Cyber Security Report (2017) observes that Universities investment in training and education plays a key role in improving understanding of Cyber security and enhances focused initiatives in developing Cyber security solutins.

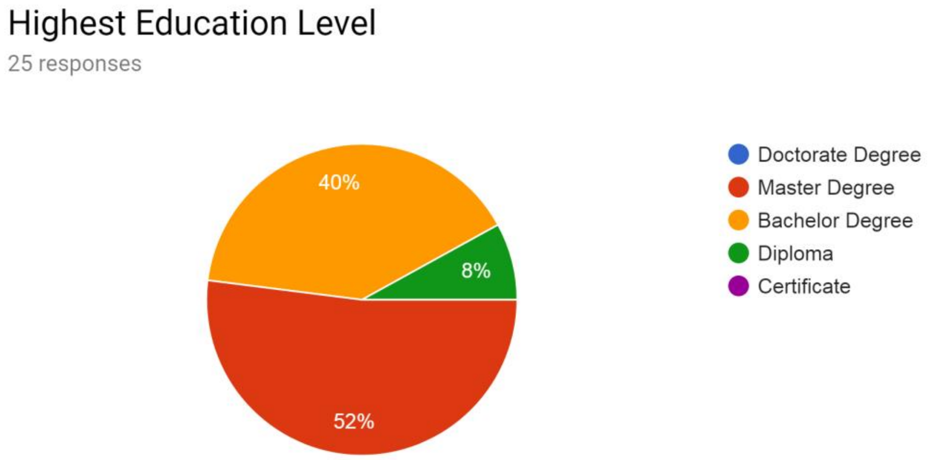


Figure 4.2: Level of Education

iv. College Posted

Data showed that a sizeable number of respondents, 18 in number (75%), come from College of Biological and Physical Sciences (CBPS). This can be attributed to the fact that the sample population who were the ICT staff belong to the ICTC which is in CBPS.

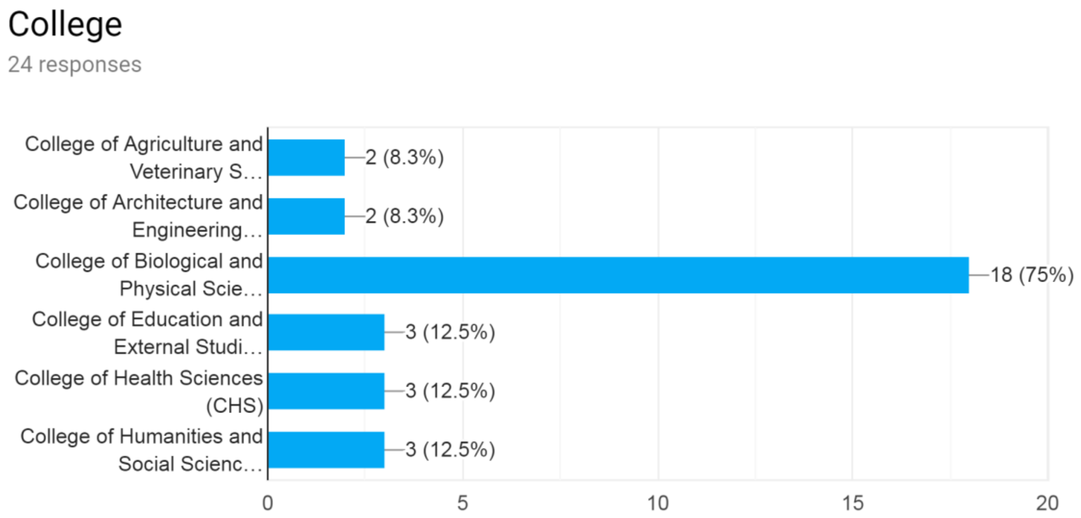


Figure 4.3: College the Respondents Belong to

v. ICT Position at the University

Figure 4.5 shows the proportions in each of the categories of participating respondents in this study. A large number of the participants were technical staff numbering 15 (60%) who comprise of IT technicians, ICT officers, technologists, system administrators, network administrators, IS officers and software developers. The members in this category are day to day staff who interact with systems and support ICT functions in the University. At the top of the ICTC Staff pyramid is the Director and Deputy Director position where 2 (8%) respondents were selected for the study. A further 5 (20%) of the respondents were various project leaders in ICTC and the remainder 3 (12%) of the respondents were Managers drawn from communications, user support and maintenance service and network and infrastructure services.

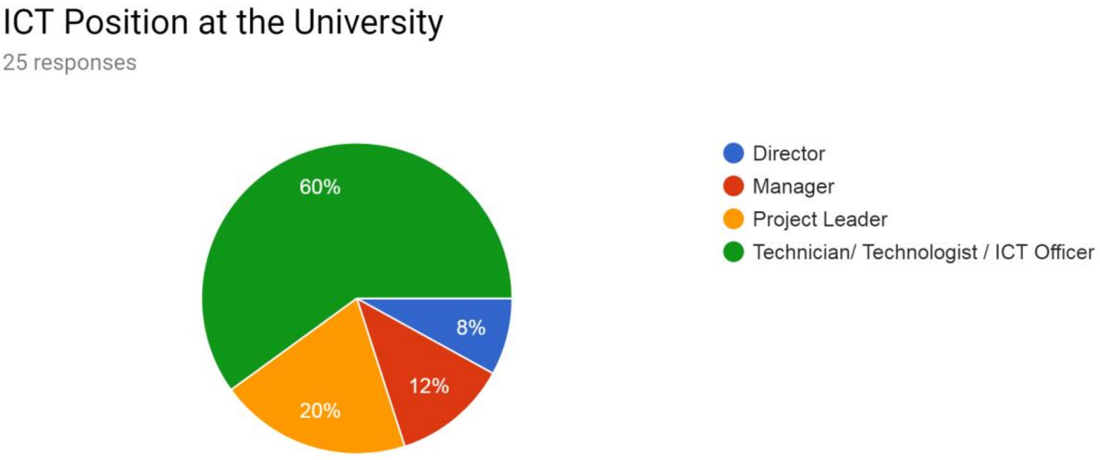


Figure 4.4: Respondents Categories

vi. Number of Years Served at the University

The study found out that over half of the study sample have worked for the university in the field of IT and ICT for 10 and above years. Figure 4.6 findings reveal that 25.9% of the respondents worked at the University for a period of between 0-7 years, 29.6% for a period between 8-12 years, another 29.5% had been in the university service for 13-20 years and a smaller sample of 18.5% of the respondents work for 20 and above years at the University.

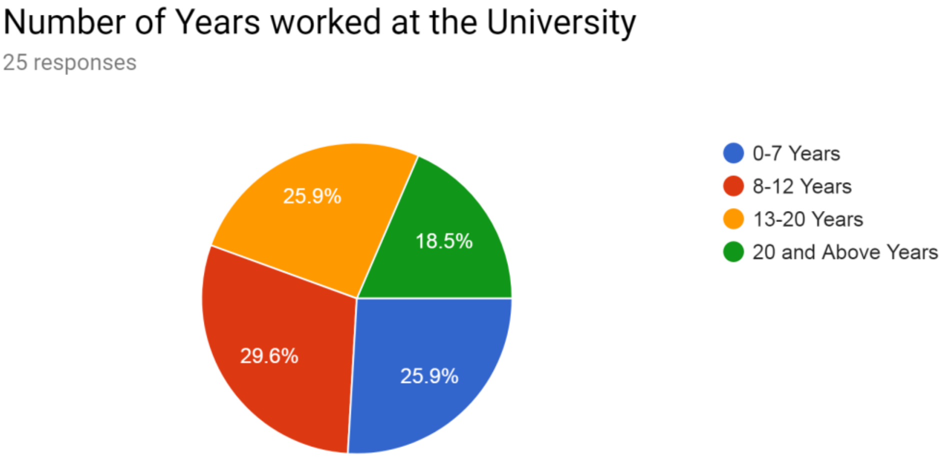


Figure 4.5: Number of Years Worked at the University

4.4 Study Variables

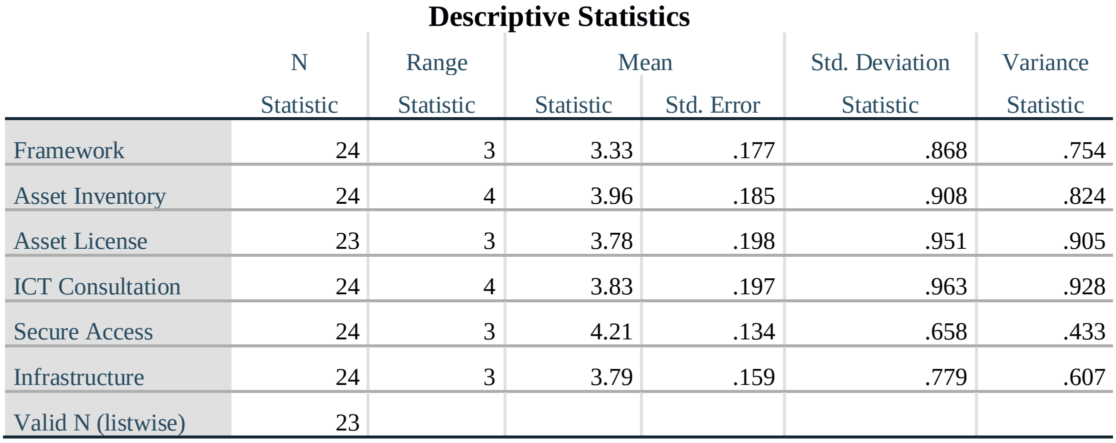
4.4.1 Findings on ICT Infrastructure Readiness

In this variable, the respondents were queried on their infrastructural readiness in matters concerning cyber security with respect to adherence of and existence of cyber security implementation frameworks and ICT assets inventory. Respondents were asked touching on secure access, data protection, involvement of ICT security specialist in database and network design, and licensing and support of network software by developers. The results shown in table 4.3 presented 75% of the respondents agreeing to ICT infrastructure having the capability to secure the institutions cyber space with a mean score of [M=3.82]. This is in agreement with ITU (2018) Global Cybersecurity index 2018 where Kenya ranked overall second in the African region and with a score of 0.110 in technical measures where infrastructural readiness is assessed.

Table 4.4.1: Infrastructure Readiness Results

		Infrastructure Readiness findings in Percentage (%)				
	Mean	**Strongly Disagree**	**Disagree**	**No Opinion**	**Agree**	**Strongly Agree**
Cybersecurity framework	3.33	0	16	40	32	8
Well maintained assets inventory	3.96	4.17	4.17	4.17	66.67	20.83
Genuine licensed ICT assets and up-to-date	3.78	0	17.39	4.35	60.87	17.39
ICT design involvement in infrastructure	3.83	4.17	8.33	4.17	66.67	16.67
Secure access for all	4.21	0	4.17	0	66.67	29.17
Infrastructural capability to serve for purpose	3.79	0	12.5	4.17	75	8.33
Overall Mean	**3.82**	**Variance**	**0.742**	**Standard Deviation**		**0.861**

Figure 4.6 shows descriptive statistics for infrastructural readiness indicator results from respondents' answers. A mean of 4.21 was computed for question regarding secure access for all users on the network whereas the question on existence of a cyber security framework scored a mean of 3.33.



Descriptive Statistics

	N	Range	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Framework	24	3	3.33	.177	.868	.754
Asset Inventory	24	4	3.96	.185	.908	.824
Asset License	23	3	3.78	.198	.951	.905
ICT Consultation	24	4	3.83	.197	.963	.928
Secure Access	24	3	4.21	.134	.658	.433
Infrastructure	24	3	3.79	.159	.779	.607
Valid N (listwise)	23					

Figure 4.6: Descriptive Statistics for Infrastructure Readiness

Globally the African region lags behind in technical field as shown in Figure 4.7. Infrastructure readiness falls under the technical field; technical indicators are founded on existing technical installations including frameworks modeled for cyber security (ITU, 2018). The elements are assessed on thebasis of number of applicable mechanisms that focus on cyber security.

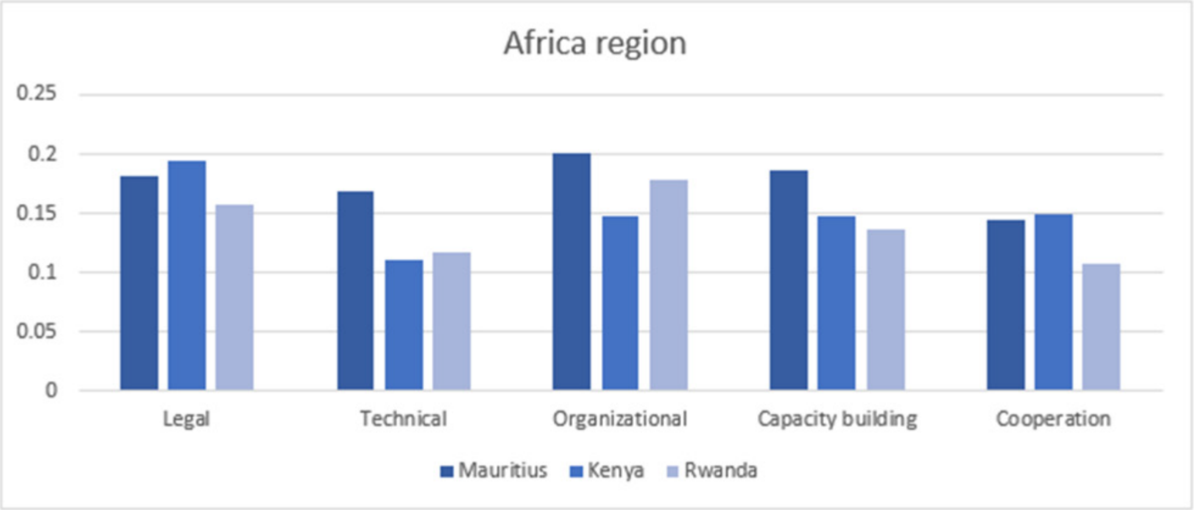


Figure 4.7: Top three ranked countries in Africa

Kenya is a leading example in the use of CIRT at the national level through involvement of ISPs, the telecommunication operators, financial organizations, content service providers critical information infrastructure providers, domain name registry providers, public listed utility, and academia like the higher learning institutions (ITU, 2018)

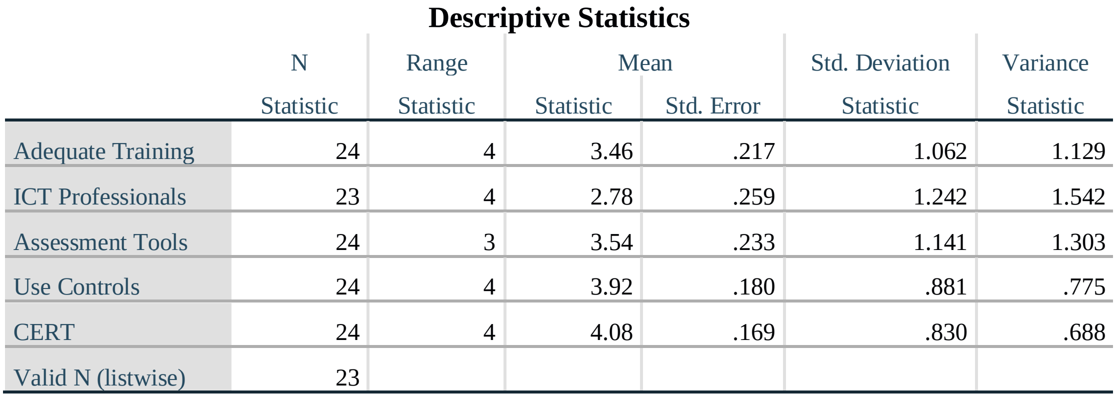
4.4.2 Findings on ICT Human Resource Readiness

This section sought to establish attributes of the respondence relating to human resource readiness to cyber security. It asked question relating to training of staff, professional merit, personnel equipped with necessary tools and ability to institute control measure and existence of a CERT to handle cyber-attacks. Table 4.4.2 exemplifies that; only 8.33% of the queried respondents strongly agree to there beening adequate training on cyber secuity matters and the existence of certified ICT security professional in their ranks to deal with cyber incidences, 70.83% agree that they are capable of executing control measures and a further 66.67% agree that a CERT will enhance the ability to secure and deal with cyber incidences in instituion.

Table 4.4.2: Human Resource Readiness Results

	Mean	**Human Resource Readiness findings in Percentage (%)**				
		Strongly Disagree	**Disagree**	**No Opinion**	**Agree**	**Strongly Agree**
Adequate training offered for all staff	3.46	4.17	20.83	8.33	58.33	8.33
Certified ICT professionals staffing	2.78	8.33	45.83	12.5	20.83	8.33
Staff provided with assessment tools	3.54	0	29.17	8.33	41.67	20.83
Ability to use controls	3.92	4.17	4.17	4.17	70.83	16.67
Computer Emergency Response Team	4.08	4.17	0	4.17	66.67	25
Overall Mean	**3.5**	**Variance**	**1.087**	**Standard Deviation**		**1.043**

Yunis and Koong (2015) agree that human resource training ensures a coordinated and comprehencive approch to the emergence of new technologies and the cyber space growth. As Shown in Figure 4.8, respondents mean score to question on existence of cyber security teams was 4.08 and a low mean of 2.78 believe that there are adequate ICT professionals in the institution to deal with cyber incidences.



Descriptive Statistics

	N	Range	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Adequate Training	24	4	3.46	.217	1.062	1.129
ICT Professionals	23	4	2.78	.259	1.242	1.542
Assessment Tools	24	3	3.54	.233	1.141	1.303
Use Controls	24	4	3.92	.180	.881	.775
CERT	24	4	4.08	.169	.830	.688
Valid N (listwise)	23					

Figure 4.8: Descriptive Statistics for Human Resource Readiness

Cheang (2009) also observed that human resource is considered as a major cyber security issue that should be used for assessment. These findings emphasize role that ICT personnel plays incyber security initiatives and their contribution to management and development of information security and the cyber space.

4.4.3 Findings on ICT Environment Readiness

The Environment indicator in this study referred to external and internal factors that affect institution's ability to deal with cyber-incidents. It sought to establish whether cyber-attacks would cause critical damage to the organization, institutions access to real-time threat intelligence, partnership with other stakeholders and agencies involved in cyber security and whether there were deliberate efforts towards promotion of awareness within and without the institution on cyber security. A favorable environment that supports cyber security progression will incentivize development of sectors in cyber security (ITU, 2018).

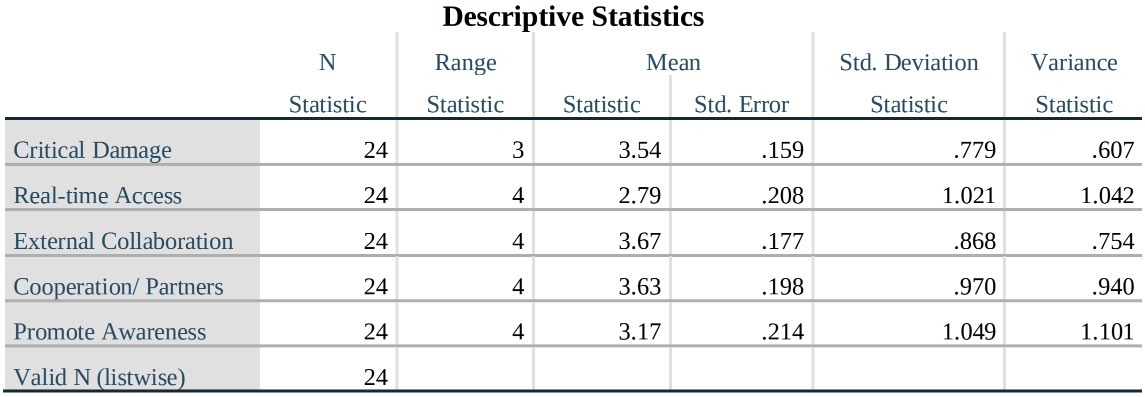
Findings on questions regarding environment as shown in Table 4.5, indicate a 66.67% of respondents agree to, an attack on the institutions network would cause critical damage, and

45.83% of them disagree that there exists real-time access by staff to threat data or intelligence. A Further 54.7% of the respondents agree that cooperation in information sharing and incidence management with partners plays a major role in the cyber security environment.

Table 4.4.3: Environment Readiness Results

	Mean	**Environment Readiness findings in Percentage (%)**				
		Strongly Disagree	**Disagree**	**No Opinion**	**Agree**	**Strongly Agree**
Cyber-attack will cause critical damage	3.54	4.17	4.17	25	66.67	0
Real-time access to threat intelligence	2.79	4.17	45.83	20.83	25	4.17
External collaboration with security agencies	3.67	4.17	4.17	20.83	62.5	8.33
Cooperation in information sharing and incidence management	3.63	4.17	8.33	20.83	54.17	12.5
Promote awareness programs internal/external	3.17	4.17	25	29.17	33.33	8.33
Overall Mean	**3.36**	**Variance**	**0.8888**	**Standard Deviation**		**0.9428**

The findings of mean values are between 2.79 and 3.67, showing respondents having similar and likeminded reaction on the responses to environment readiness. This concurs with a comprehensive study conducted in 2016 that indicated a complete set of system assessment may not be identified without the understanding of system configuration, interactions with other systems, stakeholders and in general its environment (Cherdantseva, et al., 2016). Decisions must be well informed and fashioned on basis of an in-depth knowledge of a system and its environment. Figure 4.9 gives the descriptive statistics for environmental readiness as analyzed in SPSS.



Descriptive Statistics

	N	Range	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Critical Damage	24	3	3.54	.159	.779	.607
Real-time Access	24	4	2.79	.208	1.021	1.042
External Collaboration	24	4	3.67	.177	.868	.754
Cooperation/ Partners	24	4	3.63	.198	.970	.940
Promote Awareness	24	4	3.17	.214	1.049	1.101
Valid N (listwise)	24					

Figure 4.9:Descriptive Statistics for Environmental Readiness

4.4.4 Findings on ICT Culture Readiness

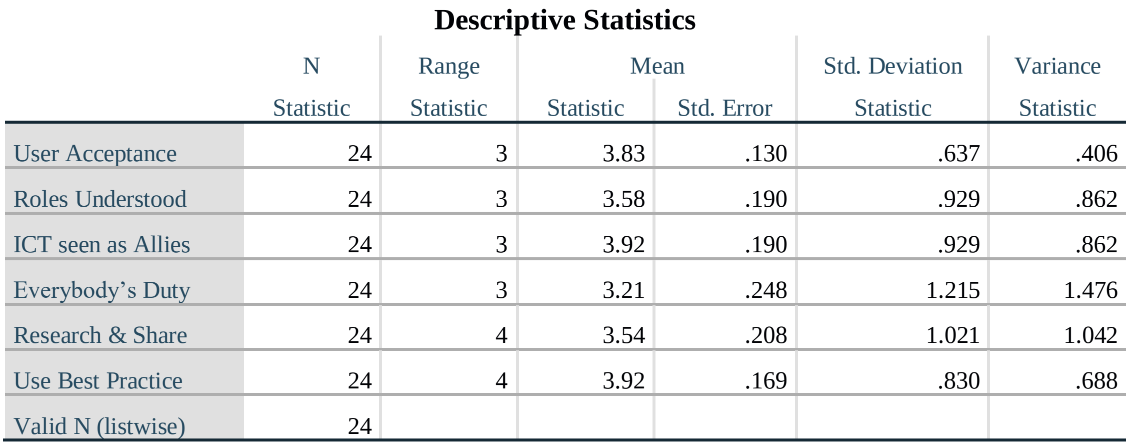
Table 4.6 results indicates views of respondents in the following; acceptance of cyber security regulation and policy by users, ease of understanding of procedures and roles, consultation of ICT by end users on cyber matters, responsibility of all users concerning cyber security, if there is research and sharing of information on security issues, if there are efforts of engaging cyber security best practices. Results here reveal a majority (91.67%) of respondents agree to, users readily accept laid cyber regulations and policy, also 79.17% agree to the use of best practices in cyber security.

Yunis and Koong (2015) referred to cultural asspects as very important factors that influence non compilace behavour by staff. The culture readiness variable had the second highest mean 3.67 with a small mean difference in the lowest mean 3.21 and the highest mean 3.92 for item regarding engaging cyber security best practices and consultation of ICT in security matters. This is in agrement with a study by Reid and Niekerk (2014) which observed that erevy user participating in ICT matters, particularly in the internet environment, need to be informed on cyber security awareness. Further, internal and external organization users are expected to be conscious of cyber security and engage information or cyber security best practices. Results of cyber safety assessment can be viewed to recognize shortcomings, focus areas, and aligning priotities in external and internal events of a security section, justify training and awareness, sharing information as well as collaborating efforts (Kaspersky Lab, 2017).

Table 4.4.4: Culture Readiness Results

	Mean	Culture Readiness findings in Percentage (%)				
		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
Users readily accept cyber regulations and policy	3.83	4.17	0	4.17	91.67	0
Easily understood security procedures and user roles	3.58	0	20.83	4.17	62.5	8.33
ICT staff are consulted, seen as allies in securing system	3.92	0	12.5	8.33	54.17	25
Cyber security is taken as everybody’s responsibility	3.21	0	45.83	4.17	33.33	16.67
Research and share information to improve	3.54	4.17	16.67	8.33	62.5	8.33
Engage CS best practices	3.92	4.17	41.7	0	79.17	12.5
Overall Mean	**3.67**	**Variance**	**0.7457**	**Standard Deviation**		**0.8635**

The use of cyber security best practice question scored a mean of 3.92 as shown in Figure 4.10. On the question of ease of understanding procedures and roles by users, a mean score of 3.58 was attained and a mean of 3.92 for question on ICT staff seen as allies in cyber security



Descriptive Statistics

	N	Range	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
User Acceptance	24	3	3.83	.130	.637	.406
Roles Understood	24	3	3.58	.190	.929	.862
ICT seen as Allies	24	3	3.92	.190	.929	.862
Everybody’s Duty	24	3	3.21	.248	1.215	1.476
Research & Share	24	4	3.54	.208	1.021	1.042
Use Best Practice	24	4	3.92	.169	.830	.688
Valid N (listwise)	24					

Figure 4.10: Descriptive Statistics for Cultural Readiness

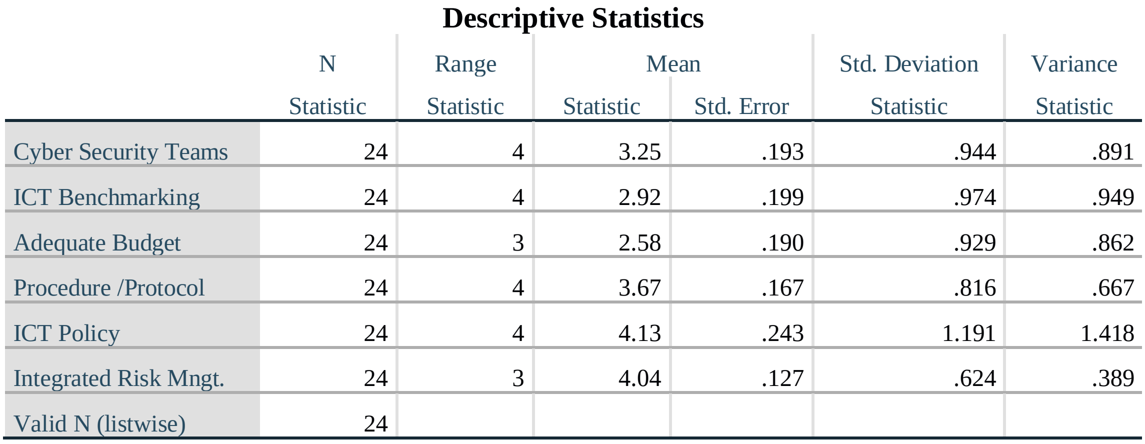
4.4.5 Findings on ICT Organization Readiness

The Table 4.4.5 shows outcomes to questions responded to concerning organizations readiness to cyber security. This includes the following areas; establishment of cyber security teams, development of ICT, budget allocation and utilization towards security concerns, existence of an ICT policy outlining guidelines and the risk management processes. Findings indicate that a majority (45.83%) disagree that cyber security operations are adequately budgeted for, 54.17% of the respondents strongly agree that there is an ICT policy outlining user services and equipment guidelines. In addition, 41.67% agree that there are established cyber security teams and 75% indicate that there is an integrated risk management process.

Table 4.4.5: Organization Readiness Results

	Mean	**Organization Readiness findings in Percentage (%)**				
		Strongly Disagree	**Disagree**	**No Opinion**	**Agree**	**Strongly Agree**
Established CS teams	3.25	4.17	16.67	33.33	41.67	4.17
ICT Benchmarking to measure development	2.92	8.33	20.83	45.83	20.83	4.17
Adequate budget to manage cyber operations	2.58	8.33	45.83	25	20.83	0
Develop procedures/ protocol and dissemination	3.67	4.17	4.17	16.67	70.83	4.17
ICT Policy outlining user guideline for services and equipment	4.13	8.33	4.17	0	33.33	54.17
Integrated risk management process for identification, protection, control, restore	4.04	0	4.17	4.17	75	16.67
Overall Mean	**3.43**	**Variance**	**0.8627**	**Standard Deviation**		**0.9288**

In figure 4.11, a high mean of 4.13 was scored for question regarding existence of an ICT policy outlining user guideline for services and equipment. Adequacy of cyber security budget scored a low mean 2.58, concurring with Fischer (2016) who identifies the need to increase cyber security funding for agencies and have revolving fund for modernizing ICT.



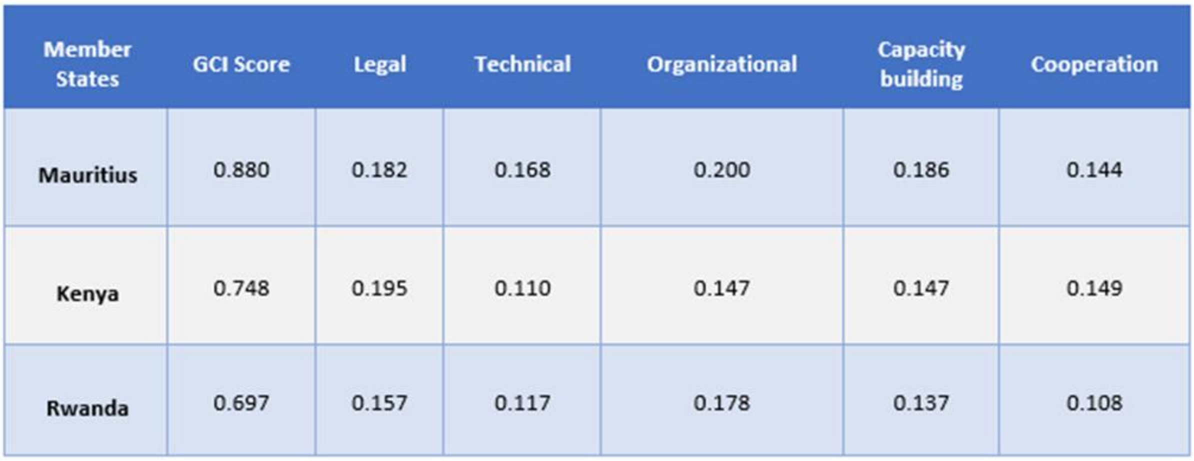
Descriptive Statistics

	N	Range	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Cyber Security Teams	24	4	3.25	.193	.944	.891
ICT Benchmarking	24	4	2.92	.199	.974	.949
Adequate Budget	24	3	2.58	.190	.929	.862
Procedure /Protocol	24	4	3.67	.167	.816	.667
ICT Policy	24	4	4.13	.243	1.191	1.418
Integrated Risk Mngt.	24	3	4.04	.127	.624	.389
Valid N (listwise)	24					

Figure 4.11: Descriptive Statistics for Organizational Readiness

Hansen (2016) observes that organizational aspects are essential for proper implementation of any initiatives. Creation of efficient organization structures is necessary for endorsing cyber security, promoting the role of monitoring and combating cyber crime. ITU (2018) ranked Kenya lowly at a score of 0.147 on organizational aspect as shown in Table 4.8.

Table 4.4.6: Top three countries in the African region



Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
Mauritius	0.880	0.182	0.168	0.200	0.186	0.144
Kenya	0.748	0.195	0.110	0.147	0.147	0.149
Rwanda	0.697	0.157	0.117	0.178	0.137	0.108

4.4.6 Findings on Cyber Security Readiness

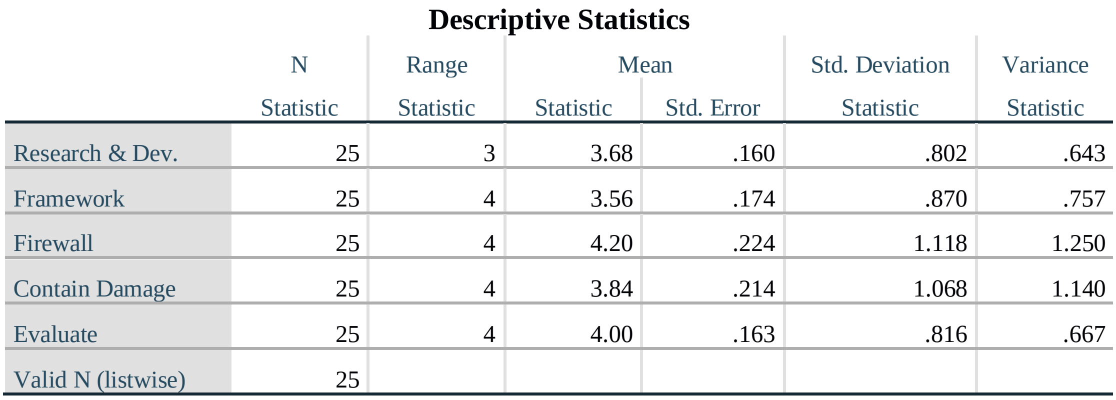
The respondent's ability and the readiness towards cyber security was examined through questions that sought to find out staff utilization of research and development programs for cyber security and if there was a well stablished cyber risk escalation framework. The use of network security controls such as firewalls and the capability to mobilize response teams and quickly contain damage was questioned. Results in Table 4.4.7 revealed that the ICT staff are indeed highly ready exuding overall mean of 3.86.

Table 4.4.7: Cyber Security Readiness Results

	Mean	**Cybersecurity Readiness findings in Percentage (%)**				
		Strongly Disagree	**Disagree**	**No Opinion**	**Agree**	**Strongly Agree**
Staff utilize R&D programs for cyber security standards/ best practices and guidelines	3.68	0	8	28	52	12
Have well established cyber risk escalation	3.56	4	8	20	64	4

framework						
Use of firewall control to protect against cyber risks	4.20	8	0	4	40	48
Capacity to rapidly contain damage and mobilize response teams	3.84	8	4	4	64	20
Ability to evaluate effectiveness of security initiatives	4.00	4	0	8	68	20
Overall Mean	**3.86**	**Variance**	**0.874**	**Standard Deviation**		**0.934**

The mean range is between 3.56–4.00 for cyber security readiness. The results indicate item on human resource readiness to be at 68% and 64% for item regarding environment readiness. The findings correspond to Cherdantseva et al. (2016) Hierachical Holographic Model (HHM) of a Supervisory Control and Data Acquisition (SCADA) system which has three dimensions: (i) hardware and software, (ii) human and (iii) environment. Figure 4.12 shows the descriptive statistics for questions related to cyber security readiness indicator.



Descriptive Statistics

	N	Range	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Research & Dev.	25	3	3.68	.160	.802	.643
Framework	25	4	3.56	.174	.870	.757
Firewall	25	4	4.20	.224	1.118	1.250
Contain Damage	25	4	3.84	.214	1.068	1.140
Evaluate	25	4	4.00	.163	.816	.667
Valid N (listwise)	25					

Figure 4.12: Descriptive Statistics for Cyber Security Readiness

4.5 Reliability and Construct Validity

The term reliability is a concept used for evaluating or testing quantitate research although it is mostly used in all forms of research. Reliability and validity testing concepts have been redefined for their usefulness in qualitative research (Golafshani, 2003). Fundamentaly, reliability denotes degree which the outcomes are consistent given a period of time, and whether these outcomes can be replicated through a comparable methodology. Construct validity refers to a determination whether the study accurately measures that aspect for which it was envisioned to aportion and subsiquent correctness of resultsof the study. IBM SPSS Statistic Subscription programme was utilized as a tool to in analysis, for testing relationship between variables, with the results as indicatd in Figures 4.13, 4.14 and 4.15.

Case Processing Summary

		N	%
Cases	Valid	25	100.0
	Excluded[a]	0	.0
	Total	25	100.0

Figure 4.13: Reliability Variables Summary

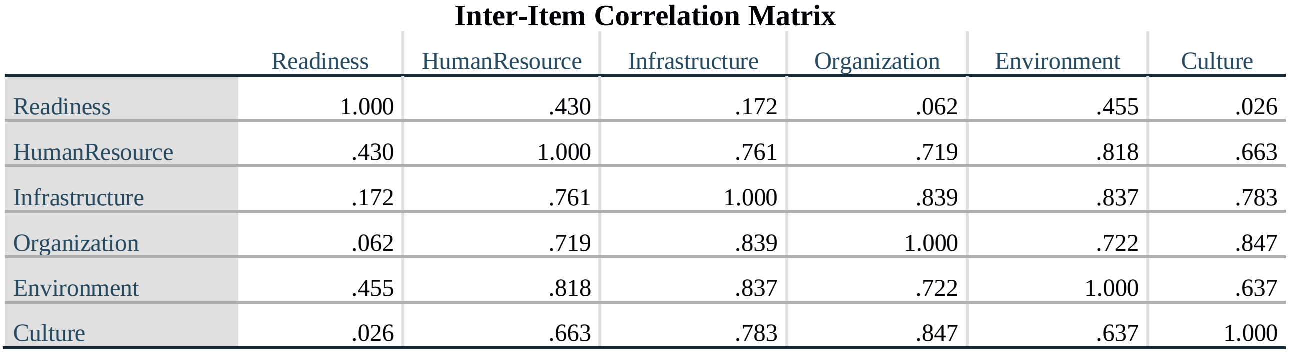
The results in the above Figure 4.13 show that zero (0) sub-variables were excluded with a case validity of all. Sekaran and Bougie (2016) observe that reliability which is less than 0.60 is considered to be poor, whereas thereliability in the range of 0.70 to be acceptable and that over 0.80 consigered good. Results in Figure 4.14 show Cronbach's alpha of well above 0.70 and most above o.80 implying that the measuring instrument was sufficiently reliable.

Reliability Statistics

.Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No of Items
.903	.894	6

Figure 4.14: Reliability Statistic

Correlations between the items is high with the least value being .637 and the highest set of correlation value at .839. Inter-item correlation of above .30 or .40 is considered to be appropriate value; the closer Cronbach's alpha is to 1, the higher the internal consistency reliability among the items (Sekaran & Bougie, 2016)



Inter-Item Correlation Matrix

	Readiness	HumanResource	Infrastructure	Organization	Environment	Culture
Readiness	1.000	.430	.172	.062	.455	.026
HumanResource	.430	1.000	.761	.719	.818	.663
Infrastructure	.172	.761	1.000	.839	.837	.783
Organization	.062	.719	.839	1.000	.722	.847
Environment	.455	.818	.837	.722	1.000	.637
Culture	.026	.663	.783	.847	.637	1.000

Figure 4.15: Inter-Item Correlation Matrix

4.6 Statistical Modeling

4.6.1 Linear Regression

A linear regression analysis was undertaken so as to determine factors which influence cyber security readiness, also to test the CSR model developed. Linear regression method models that relationship between the scalar variable denoted as y and another or extra variables denoted as x. IBM SPSS Statistic Subscription programme was used as a tool for this analysis. A scatter plot was generated for each variable to highlight the kind of relationship that exists amongst dependent variable and every independent variable.

ICT Infrastructure

Visual examination of the scatter plot for ICT infrastructure suggests a positive linear relationship with cyber security readiness. This implies that the better the infrastructure the better security.

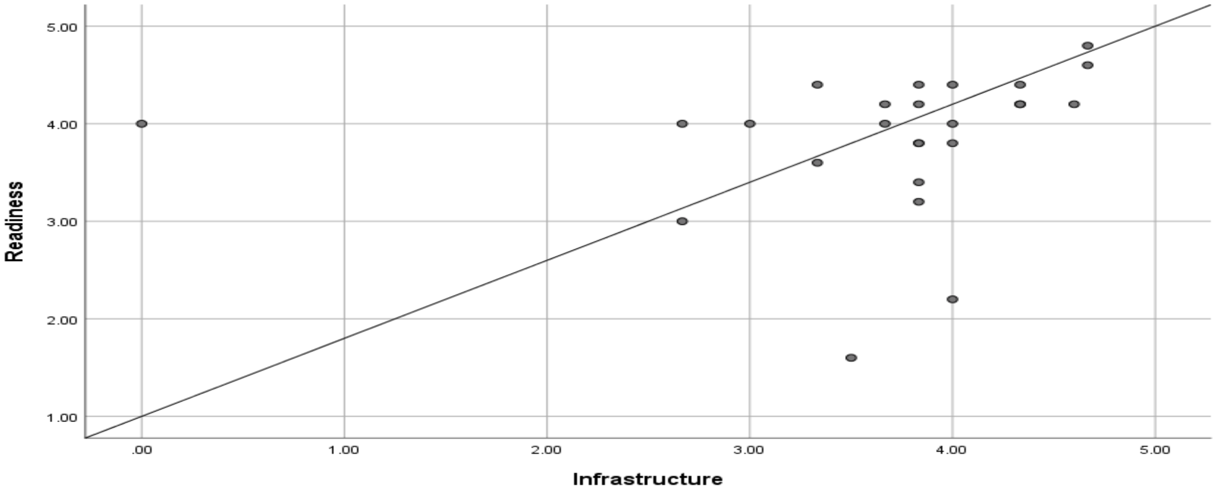


Figure 4.16: Scatter Plot of Readiness/ICT Infrastructure

ICT Human Resource

A visual examination of the ICT human resource scatter plot points to the fact that there exists a strong positive linear relationship with cyber security readiness.

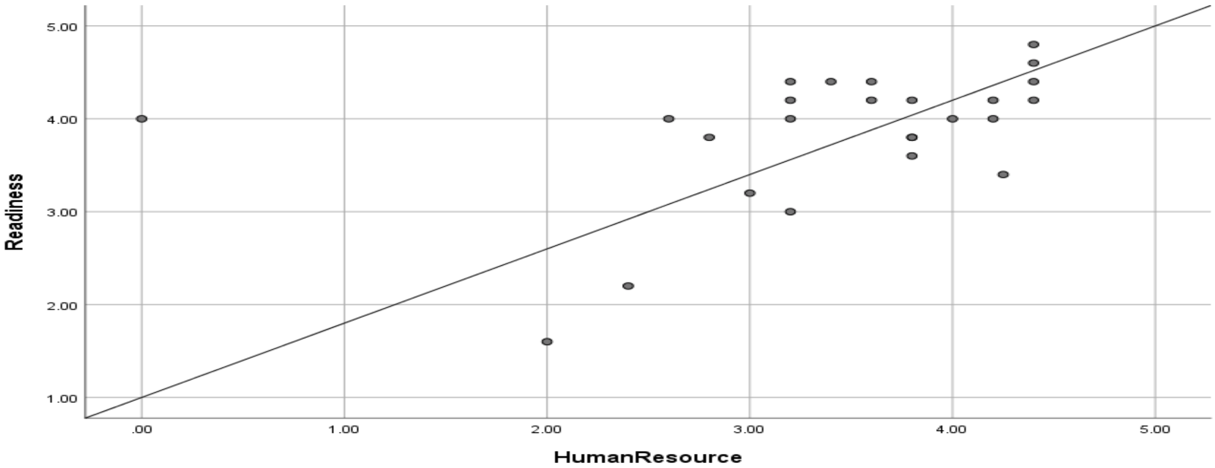


Figure 4.17: Scatter Plot for Readiness/ ICT Human Resource

The visual examination of the scatter plot for ICT environment suggests a very strong positive linear relationship with cyber security readiness.

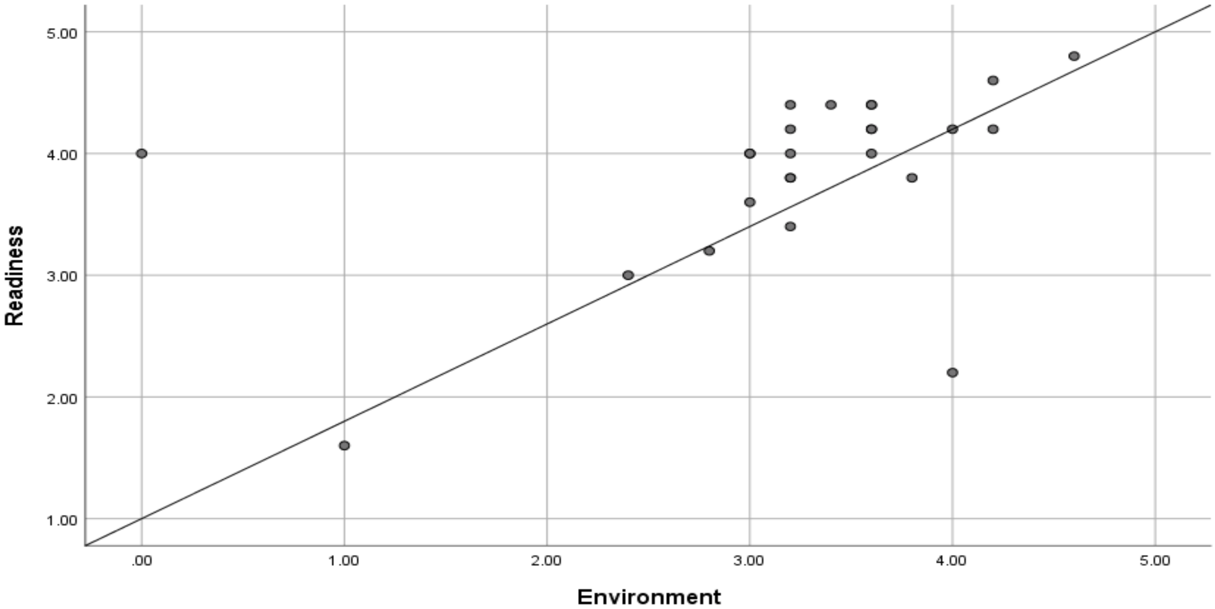


Figure 4.18: Scatter Plot of Readiness/ ICT Environment

A visual examination of the scatter plot for ICT Culture suggests that there is a positive relationship with cyber security readiness, however not that strong.

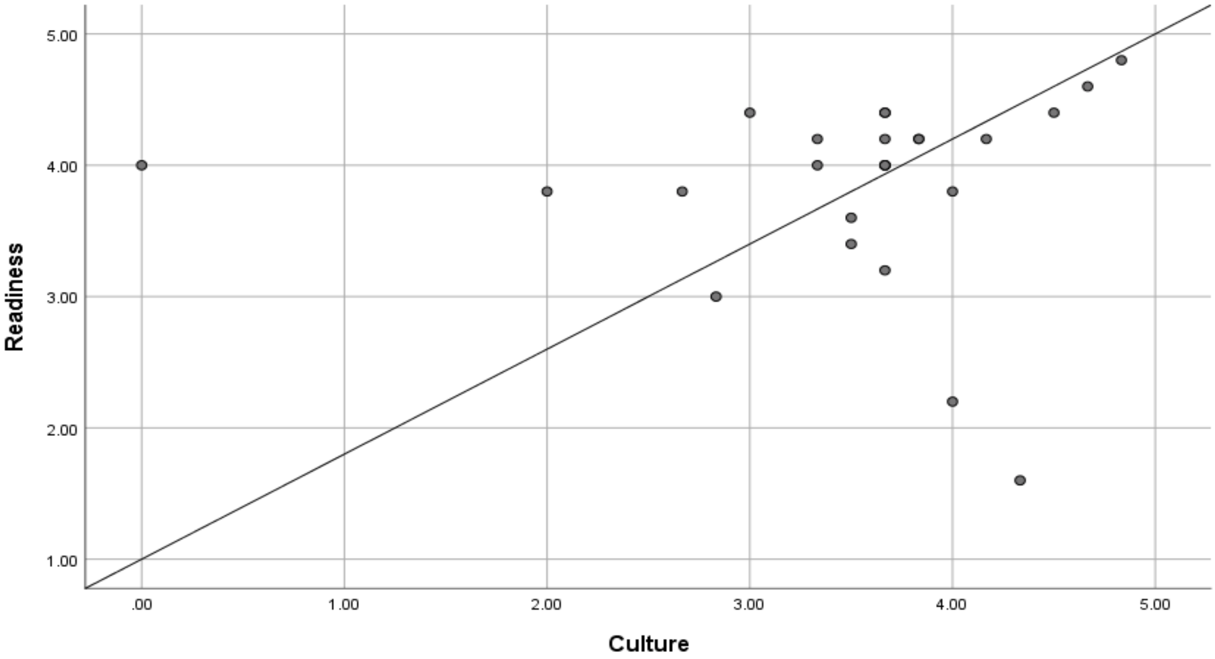


Figure 4.19: Scatter Plot for Readiness/ ICT Culture

A Visual examination of the ICT Organization scatter plot suggests a positive relationship with cyber security readiness although not as strong.

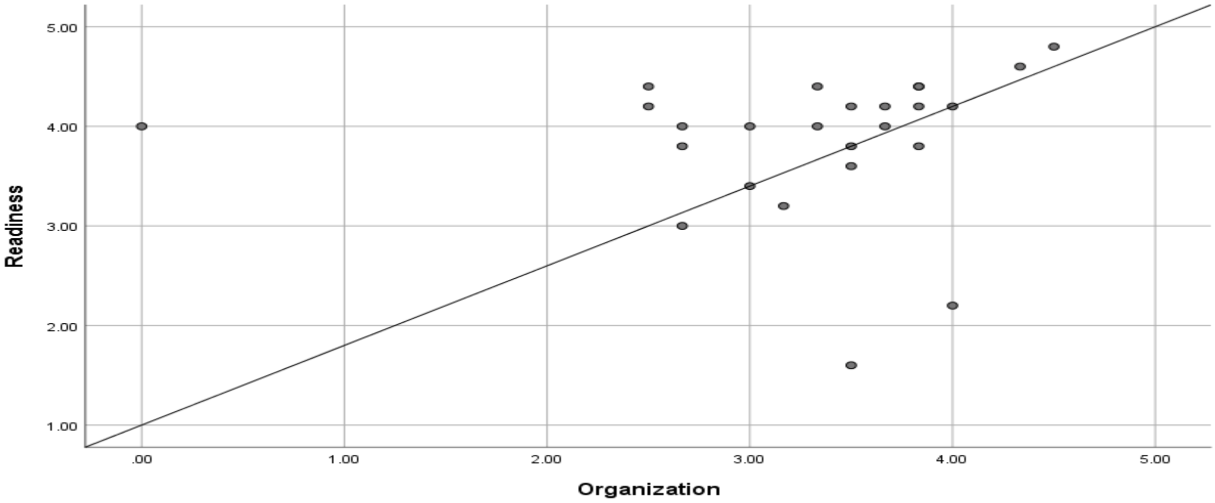


Figure 4.20: Scatter Plot of Readiness/ ICT Organization

4.7 Model Summary

Below are summary results from the model

Table 4.7.1: Model Summary

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.674[a]	.455	.311	.60143

a. Predictors: (Constant), Culture, Environment, Human Resource, Organization, Infrastructure

b. Dependent Variable: Cyber Security Readiness

The regression analysis shows a relationship, R = 0.674 and $R^2 = 0.455$ which means that 31.1% of the corresponding changes in Cyber Security Readiness can be explained by a unit increase in Culture Environment, Human Resource, Organization and Infrastructure.

An analysis of Variance (ANOVA) in this study was used to examine suitability of developed model for this study. Significance value is 0.030, which is less than o.o5 hence the CSR assessment model shows statistically significance in predicting cyber security readiness.

Table 4.7.2: ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.729	5	1.146	3.168	.030[b]
	Residual	6.873	19	.362		
	Total	12.602	24			

a. Dependent Variable: Cyber Security Readiness

b. Predictors: (Constant), Culture, Environment, Human Resource, Organization, Infrastructure

A further test on the model indicate a positive beta coefficient for two independent variables and negative beta coefficient for three. The cyber security readiness is at 3.342 with human resource, infrastructure, organization environment and culture readiness at a constant of Zero.

Table 4.7.3: Coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.342	.518		6.446	.000	2.257	4.427
	Human Resource	.350	.233	.472	1.504	.149	-.137	.838
	Infrastructure	-.317	.317	-.409	-.999	.331	-.981	.347
	Organization	-.298	.313	-.362	-.951	.354	-.954	.358
	Environment	.574	.274	.766	2.098	.050	.001	1.148
	Culture	-.112	.252	-.148	-.443	.663	-.638	.415

a. Dependent Variable: Cyber Security Readiness

Findings of the analyzed data infer; keeping the rest of the independent variables at the zero mark, an upsurge to human resource readiness by a unit will result into a 0.350 increase in cyber security readiness, by increasing environmental readiness with one unit, it will result into a 0.574 increase in cyber security readiness.

The findings show the level of confidence 95%, human resource readiness with 0.149 significance level, infrastructure readiness with 0.331, organization readiness with 0.354, environment readiness had 0.050, whereas culture readiness level of significance was at 0.663. The most significant factor to Cyber Security Readiness Assessment points to the environment factor, after which the human resource factor follows.

Table 4.7.4: Descriptive Statistics

Descriptive Statistics

	Mean	Std. Deviation	N
Cyber Security Readiness	3.8560	.72461	25
Human Resource	3.4260	.97693	25
Infrastructure	3.6707	.93439	25
Organization	3.2933	.88097	25
Environment	3.2240	.96664	25
Culture	3.5200	.96023	25

4.8 Discussion of Findings

4.8.1 Cyber Security Readiness

Findings in this study show that a greater number of the respondents are cyber security ready [M=3.86]. Furthermore, the personnel have the ability to evaluate effectively the security initiatives [M=4.0], the environment within which the University operates in is protected with controls such as firewall [M=4.20] and the ICT response teams can be rapidly mobilized and contain damage [M=3.84]. This finding is supported by Department of Energy (2014) research that observes that enhanced skill sets of an organization’s workforce and having personnel with approprate levels of cyber security experience, education and training is critical for cyber security. Further, acknowleding increased organizations’ reliance on advanced technology for digital control and communications, the ICT human resource issues are a critical aspect of successfully addressing cyber security and risk manament of systems.

4.8.2 Factors Influencing Cyber Security Readiness

Majority of the respondents, as revealed by the study, are confidently in agreement that environmental readiness indeed is the greatest critical factor in CSR, with 66.67% indication that a cyber-attack would cause critical damage. They however note that in the organization factor, funding is inadequate (45.83%) to support ICT efforts and operations in securing the systems. Majority of the respondents (70.83%) indicated their ability as human resource to manage cyber security operations and apply controls [M=3.92], but a good number (45.83%) disagree that there are enough certified ICT professionals among their ranks [M=2.78]. Infrastructure readiness tested for existence of; cyber security framework, a well-maintained ICT assets inventory, licensing and update of assets, involvement of ICT in infrastructural development, secure access for all users and the fit for purpose of the infrastructure. The results indicated that there is a cyber security framework for ICT resources [M=3.33], assets inventory is well maintained [M=3.96] and majority of the respondents are confident that the infrastructure provides for secure access for all [M=4.21]. However, lack of genuine licensing of ICT assets and updating could be pose a challenge to effectively secure the systems [M=3.78].

4.8.3 Cyber Security Readiness Developed Model

Cyber security readiness proposed model bares five independent distinct factors; ICT infrastructure, ICT human resource, ICT Culture, ICT Organization and ICT Environment. The outcomes of the linear regression analysis reveal a 45.5% respondents cyber security readiness level. Evidently, this indicates to the possibility of there being other variables which are not considered in this study and are part of what may influence cyber security readiness. The Cultural factor [0.663], organization [0.354], infrastructure [0.331] show little or no significance to the ICT personnel's cyber security readiness. Nevertheless, the cyber security model developed can be considered statistically significant, having an F value of 0.030. The model could therefore be useful in predicting the respondents' cyber security readiness.

CHAPTER FIVE

5 RECOMMENDATEIONS, CONCLUSIONS AND SUMMARY

5.1 Introduction

Researcher in this study pursued to assess the cyber security readiness of higher learning institutions in Kenya through a cross sectional survey of University of Nairobi. Specifically, the study looked at infrastructure readiness, human resource readiness, environment readiness organization readiness and culture readiness. This chapter gives a summary of the data collected, each statistical handling of analysis through discussing the specific study objectives, interpreting and evaluating results. Conclusions observed here are point-to-point relate to the specific study objectives. The chapter's recommendations discuss further studies to be considered, or a propose in changing of the conclusion observed.

5.2 Findings Summary

Empirical literature revealed the ability to securely connect to the network and online or virtually to a system is imperative to safety and supporting learning and training environments. Literature further showed that in higher learning institutions, there is open environment for network access, and digital platforms are increasingly being adopted by students in learning. Visitors, faculty and support staff are regularly accessing, retrieving, and cooperating online. Further, the administrative and managerial functions are operated online either remotely or onsite. Unfortunately, the open environment has made higher learning institutions vulnerable and easy targets for cyber-attacks.

In this study, there were three objectives; to develop a model for the assessment of cyber security readiness, to conduct a diagnostic cyber security readiness assessment, finally to carry out a determination of the factors that influence cyber security readiness to Kenyan higher learning institutions. Homogeneous sampling method was in this study put to use in the participants of this work who were purposively selected for a census. Resultantly, the use of descriptive statistics aimed at analyzing the collected data via questionnaires as the primary collection instrument. The instrument was tested and analyzed for validity and reliability using a formula of Cronbach's Coefficient Alpha. Use of ANOVA tested the suitability of developed model in this research. SPSS Statistic Subscription version provided a statistical tool for analysis all through.

From this research, a cyber security readiness assessment model was developed and consiquently the outcomes of analysis revealed that the model to a great extent is statistically significant. This is to say that the model can be used as a tool to measure cyber security readiness iin higher learning institutions. The results show that environmental readiness as the most important factor folowed by human resource readiness. The cultural, organization and infrastructure factors showed little or no significance in the cyber security readiness of the ICT personnel. However, whereas the findings indicated the human resource readiness as high, certified cyeber security professional where very few and that the staff where not provided with suitable assessment tools for cyber security.

5.3 Conclusions

Guided by these findings, cyber security readiness assessment model developed explains 45.5% of the respondent's cyber security readiness. In this study, environment readiness and human resource readiness were identified as factors that highly influence to a large extent the ICT staff cyber security readiness. In Addition, the research identified areas of improvement in; organization factor like inadequate funding of ICT operations; cultural factor the need for sensitization of users to consider cyber security as everybody's responsibility and not only for ICT staff; and infrastructure factor to enhance secure access. The higher learning institutions should therefore put more emphasis cyberspace safety and security for its critical infrastructure. This is in agreement with the observations of ITU (2018) and DOE (2014) on the need for cyber security policies that take ito consideration the importance of cyberspace safety; support private nad public partnerships, build user awareness, empower human capital to identify cybersecurity problems, participation of technical staff in designing solutions and sharing with users the responsibility for having safe and resilient cyberspace.

This study does not cover the entire universe of cyber security readiness of Kenya's higher learning institutions, since the studies sample that was taken for consideration was only that of the ICT staff. The model can nonetheless be used to provide insight to the cyber security readiness of other institutions since it is statistically significant.

5.4 Recommendations

The study justifies that, having personnel who are well trained, have the required tools of operation, are adequately funded, engage in best practices and operate in an enabling environment have a good understanding of the dynamics of cyber security to enable the safeguarding of the cyberspace in higher learning institutions. Specifically, the study recommends:

The university management should greatly improve funding for ICT operations and make considerable budgeting for cyber security since safeguarding the cyberspace is not a finite task, rather a series of interrelates, ongoing processes. The provision of adequate cyber security resources should not be an afterthought but should inform every step of the process.

Users and administrators of the ICT resources require cyber security awareness and training program to communicate security requirements and appropriate behavior. The program should be aimed to provide training on use of information and computing resources in a protective, efficient, ethical and lawful manner.

5.5 Limitations of the Study

The research findings cannot be subjected directly to the case of other higher learning institutions owing to the fact that these institutions differ in levels of readiness for the various factors listed in the study.

5.6 Suggestions for further Studies

Due to the constraints highlighted in the first chapter; exploring the cyber security readiness of ICT functions and staff, this study could not exhaust all the parameters needed to assess cyber security readiness of higher learning institutions in Kenya. The perceptions of University management, faculty, students and visitors were not captured; therefore, factors for assessing cyber security readiness of these groups of people need to be established. Other factors like legal measures, regulations and economic aspect, just to mention a few, require further investigation on how significant they are to cyber security readiness.

REFERENCES

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K. & Oluwadare, S. A., 2017. A Review of Game Theory Approach to Cyber Security Risk Management. *Nigerian Journal of Technology (NIJOTECH),* 36(4), pp. 1271-1285.

Armstrong, R. C., Mayo, J. R. & Siebenlist, F., 2009. *Complexity Science Challenges in Cybersecurity,* Livermore, California: Sandia National Laboratories.

Babbie, E., 2010. *The Practice of Social Research.* 12th ed. Belmont, CA: Wadsworth Cengage Learning.

Banerjee, A. & Chaudhury, S., 2010. Statistics without tears: Populations and samples. *Industrial psychiatry journal,* Volume 19. 60-5.

Baskarada, S., 2014. Qualitative Case Study Guidelines. *The Qualitative Report,* 19(40), p. 4.

Battaglia, M. P., 2011. *Encyclopedia of Survey Research Methods.* Thousand Oaks: Sage Publications.

Bernard, H. R., 2011. *Research Methods in Anthropology: Qualitative and Quantitative Approaches.* 5th ed. Walnut Creek, California: AltaMira Press.

Castano, C., 2011. Understanding Women’s Presence in ICT: the Life Course Perspective. *International Journal of Genger, Science and Technology,* 3(2), pp. 364-386.

Cheang, S., 2009. *Conceptual Model for Cybersecurity Readiness Assessment for Public Institutions in Developing Country: Cambodia.* Seoul, Korea, Fourth International Conference on Computer Sciences and Convergence Information Technology.

Cherdantseva, Y. et al., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security,* Volume 56, pp. 1-27.

Cooper, D. R. & Schindler, P. S., 2014. *Business Research Methods.* 12 ed. New York: McGraw-Hill.

Creswell, J. W., 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 4 ed. Los Angels: SAGE.

Cwele, S., 2017. *A Baseline Study on Cybersecurity Readiness,* Pretoria, South Africa: Department of Telecommunications and Postal.

Department of Energy, 2014. *Cybersecurity Capability Maturity Model Version 1.1*, DC: DOE.

Fischer, E. A., 2016. *Cybersecurity Issues and Challenges: In Brief*, DC: Congressional Research Service.

Fowler, F. J., 2014. *Survey Research Methods.* 5th ed. Thousand Oaks, California: SAGE Publications.

Gay, L. R., Mills, G. E. & Airasian, P., 2012. *Educational Research : Competencies for Analysis and Application.* 10 ed. New Jersey: Pearson Education.

Gehem, M., Usanov, A., Frinking, E. & Rademaker, M., 2015. *Assessing Cyber Security: A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks* , Lange Voorhout: The Hague Centre for Strategic Studies.

Gercke, M., 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* s.l.: International Telecommunication Union.

Golafshani, N., 2003. Understanding Reliability and Validity in Qualitative Research. *The Qualitative Repor*, 8(4), pp. 597-606.

Hansen, R., 2016. *Cyber Security Capability Assessment*, Estonia: Tallin.

Hathaway, M. et al., 2015. *Cyber Readiness Index 2.0*, Arlington, VA: Potomac Institute for Policy Studies.

ITU, 2012. *Readiness assessment report for establishing a national CIRT*, Bangkok: International Telecommunication Union.

ITU, 2017. *Global Cybersecurity Index, Conceptual Framework*, Dubai, United Arab Emirates: International Telecommunication Union.

ITU, 2018. *Global Cybersecurity Index 2018,* London, UK: International Telecommunications Union.

Jackson, S. L., 2009. *Research Methods and Statistics: A Critical Thinking Approach.* Fourth ed. Jacksonville: Wadsworth/Cengage Learning.

Kaspersky Lab, 2017. *CyberSafety Culture Assessment*, UK: CEB/SHL.

Kenya , 2014. *Public Service Seperannuation Scheme ACT,* NAirobi, Kenya: National Council for Law.

Kenya Cyber Security Report, 2017. *Demystifying Africa's Cyber Security Poverty Line,* Nairobi, Kenya: Serianu.

Kothari, C. R., 2004. *Research Methodology: Methods and Techniques.* Second Revised ed. New Delhi: New Age International.

McClelland, R., 2009. *Cyber Security Strategy.* Australia, Commonwealth of Australia.

Mello, S., 2018. *Data Breaches in Higher Education Institutions,* New Hampshire, Durham: Spring.

Muthaura, S., Mugambi, Ayugi, C. & Njonjo, W., 2017. *Getting the Deal Through - Pensions & Retirment.* 5th ed. London: Law Business Research.

Neuman, W. L., 2011. *Social Research Methods: Qualitative and Quantitative Approaches.* Seventh ed. Boston: Allyn & Bacon Publishers.

Oketch, H. A., Wausi, A. N. & Njihia, J. M., 2014. E-Learning Readiness Assessment Model In Kenyas' Higher Education Institutions: A Case Study Of University Of Nairobi. *International Journal of Scientific Knowledge,* November.5(6).

PwC, 2014. *PwC's Cyber Readiness Health Check.* [Online] Available at: www.pwc.com [Accessed 15 May 2017].

Rahat, S., 2014. Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges. *International Journal of Emerging Trends & Technology in Computer Science,* Volume 3, pp. 233-236.

Reddy, G. N. & Reddy, G. U., 2014. *A Study Of Cyber Security Challenges And Its Emerging Trends In Latest Technologies,* Hyderabad, India: Osmania University.

Reid, R. & Niekerk, J. V., 2014. *From Information Security to Cyber Security Cultures: Organizations to Societies,* Port Elizabeth, South Africa: IEEE.

Ryoo, J., Girard, T. & E., C., 2009. *An Information Systems Security Readiness Assessment for Municipalities in Rural Pennsylvania,* Altoona: Pennsylvania State University.

Safianu, O., Twum, F. & Hayfron-Acquah, J. B., 2016. Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. *International Journal of Computer Applications,* 143(5), pp. 8-14.

Sekaran , U. & Bougie, R., 2016. *Research Methodsfor Business: A Skill-Building Approach.* 7th ed. Chichester, West Sussex, United Kingdom: John Wiley & Sons Publishers.

Staiger, C., 2017. *TIG.* [Online] Available at: https://www.tig.co.uk/blogs/women-technology-sector-dominated-men/ [Accessed 24 April 2019].

Toews, V., 2010. *Canada Cyber Security Strategy,* Canada: Government of Canada.

Tomte, C., 2011. Challenging Our Views on ICT, Gender and Education. *Nordic Journal of Digital Literacy,* 6(Special Issue), pp. 309-325.

Waithaka, S., 2016. *Factors Affecting Cyber Securityin National Government Ministries in Kenya,* Nairobi: University of Nairobi.

Wang, E. K., Ye, Y. & Xu, X., 2010. *Security Issues and Challenges for Cyber Physical Systems.* Shenzhen, China, Harbin Institute of Technology Shenzhen Graduate School.

Yin, R. K., 2014. *Case Study Research Design and Methods.* 5th ed. Thousand Oaks: SAGE Publications, Inc.

Yunis, M. M. & Koong, S. K., 2015. *A Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework.* Puerto Rico, s.n.

Zukunft, A. P. F., 2015. *Cyber Strategy,* Washington D.C.: United States Coast Guard.

APPENDICES

Appendix I : Questionnaire

The purpose of this research survey is to examine the existing cyber security influences in Kenya’s higher learning institutions and determine their readiness for cyber security. Questionnaire is designed to assist in collecting data to determine cyber security readiness through ICT personnel in the University of Nairobi. Please respond to all questions to the best of your availability. Findings of this research are solely for academic purposes and hence all responses are highly treated with confidentiality

SECTION A: RESPONDENTS DEMOGRAPHIC DETAILS

1. **Gender**

□ Male □ Female

2. **Highest Education Level**

□ Doctorate Degree

□ Master Degree

□ Bachelor Degree

□ Diploma

□ Certificate

3. **College**

□ College of Agriculture and Veterinary Sciences (CAVS)

□ College of Architecture and Engineering (CAE)

□ College of Biological and Physical Sciences (CBPS)

□ College of Education and External Studies (CEES)

□ College of Health Sciences (CHS)

□ College of Humanities and Social Sciences (CHSS)

4. **ICT Position at the University**

□ Director

□ Manager

□ Project Leader

□ Technician/ Technologist / ICT Officer

5. **Number of Years Work in the University**

□ 0-7

□ 8-12

□ 13-20

□ 20 and Above

SECTION B: CYBER SECURITY READINESS		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
i.	There is any officially recognized ICT-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines for application	□	□	□	□	□
ii.	Existence of a well-established cyber risk escalation framework that includes risk appetite and reporting threshold	□	□	□	□	□
iii.	Effective controls to protect the institution against third party cyber risks (e.g. firewalls)	□	□	□	□	□
iv.	Capacity to rapidly contain damages and mobilize response teams to cyber incidents	□	□	□	□	□
v.	Ability to evaluate the effectiveness of cyber security initiatives of the institution.	□	□	□	□	□

SECTION C: HUMAN RESOURCE READINESS		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
i.	Adequate training on cyber security issues provided to staff who lack the skills or have special requirements for ICT services	□	□	□	□	□
ii.	The institution has enough ICT professionals certified under internationally recognized certification programs in Cyber security	□	□	□	□	□
iii.	Available tools to conduct risk and vulnerability assessment and prevent attacks	□	□	□	□	□

iv.	Capability to deploy data protection controls (e.g. encryption and endpoint security)	□	□	□	□	□
v.	Ability to provide assistance, such as a help desk, Computer Emergency Response Team (CERT) in response to incidences	□	□	□	□	□

SECTION D: INFRASTRUCTURE READINESS		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
i.	There is any institutional officially-approved cyber security frameworks for implementing internationally recognized cyber security standards	□	□	□	□	□
ii.	ICT Asset inventory is maintained and kept current (e.g., physical devices, systems, software platforms and applications	□	□	□	□	□
iii.	The assets have genuine licensed copies of software for secure access, use and distribution of data.	□	□	□	□	□
iv.	Database system and computer network within the institution has been designed with consultation with the ICT security experts	□	□	□	□	□
v.	There is secure access for users of the ICT infrastructure to protect data and devices	□	□	□	□	□
vi.	Has technological infrastructure and competencies to effectively engage in cyber security	□	□	□	□	□

SECTION E: ORGANIZATION READINESS		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
i.	There is Computer Emergency Response Team (CERT) with sufficient technical capability	□	□	□	□	□
ii.	There are officially recognized ICT-specific bench marking exercises or referential used to measure cyber security development	□	□	□	□	□
iii.	Has enough budget to effectively manage daily cyber security operation and assets	□	□	□	□	□
iv.	Develop procedures and protocol for the dissemination of incident management information to respective teams	□	□	□	□	□
v.	Has an ICT policy outlining user guideline for ICT equipment and services	□	□	□	□	□
vi.	Develop an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity	□	□	□	□	□

SECTION F: ENVIRONMENTAL READINESS		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
i.	Internal critical information infrastructure damage to the institution in case of a cyber-attack	□	□	□	□	□
ii.	Real-time access to global threat intelligence (adversaries, IP reputation, security trends) that enables proactive management of	□	□	□	□	□

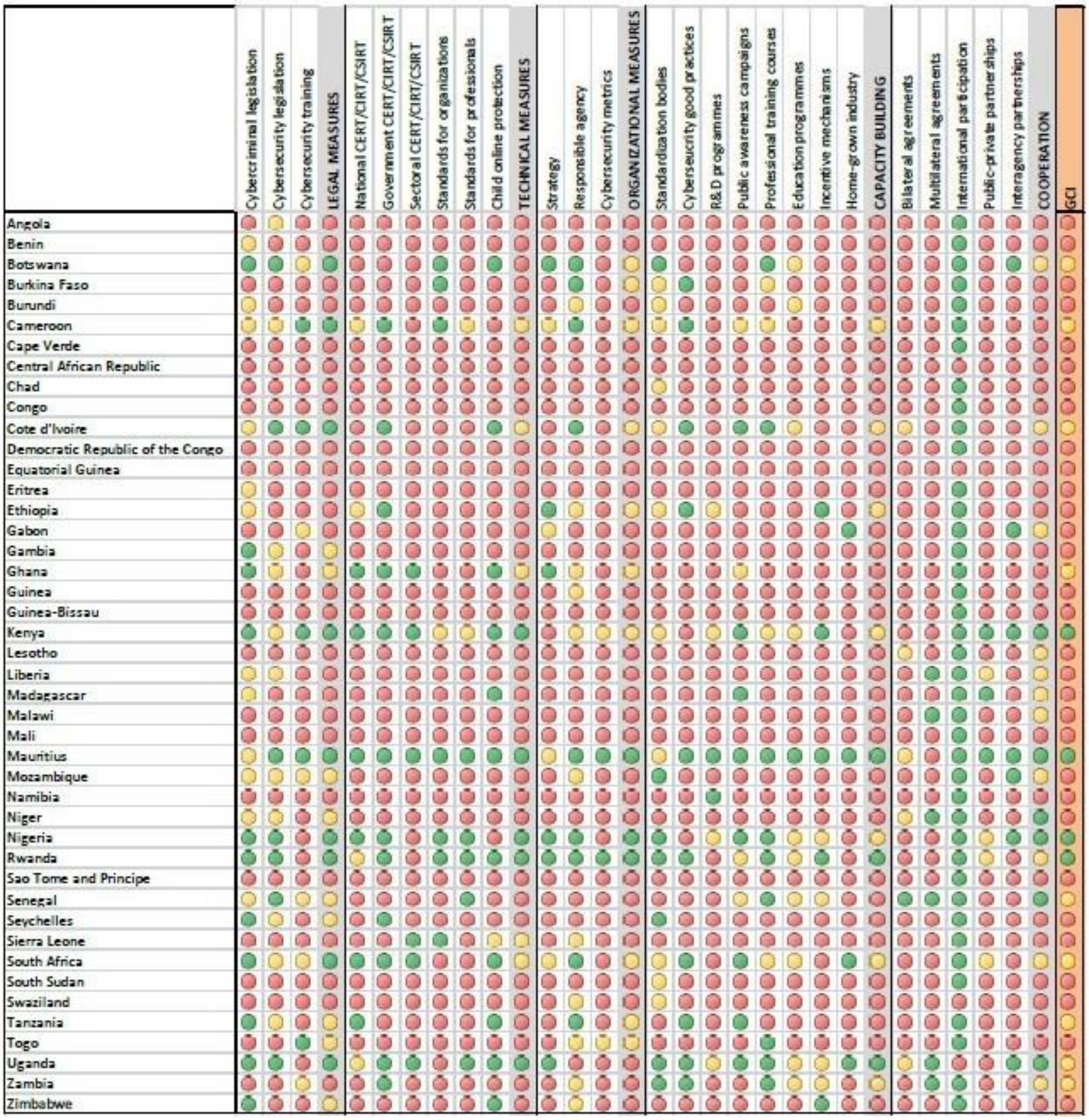
	emerging threats before they strike					
iii.	There is collaboration of institution in cyber security concerns with other Agencies	□	□	□	□	□
iv.	Establish cooperative arrangements between institution, government and other partners for information sharing and incident management	□	□	□	□	□
v.	Participates in the promotion of a comprehensive national awareness program so that all participants could secure their own parts of cyberspace and participate effectively in a new culture of cyber security	□	□	□	□	□

SECTION G: CULTURE READINESS		Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
i.	Accept safety regulations and policies as reasonable and not overly restrictive	□	□	□	□	□
ii.	Procedures and roles are well understood for promoting cyber security culture	□	□	□	□	□
iii.	Non-technical employees see ICT staff as allies and partners: encouraged to ask for help and report breaches timely	□	□	□	□	□
iv.	Cyber security is seen as everybody’s responsibility not primarily ICT in the institution.	□	□	□	□	□
v.	Staff research and share information on cyber security trends to improve knowledge base	□	□	□	□	□
vi.	Engage best practice in responding, protection, and recovery from cyber incidents	□	□	□	□	□

Appendix III: Africa Region Scorecard

Global Cybersecurity Index 2017

Figure 6.1.2: Africa region scorecard

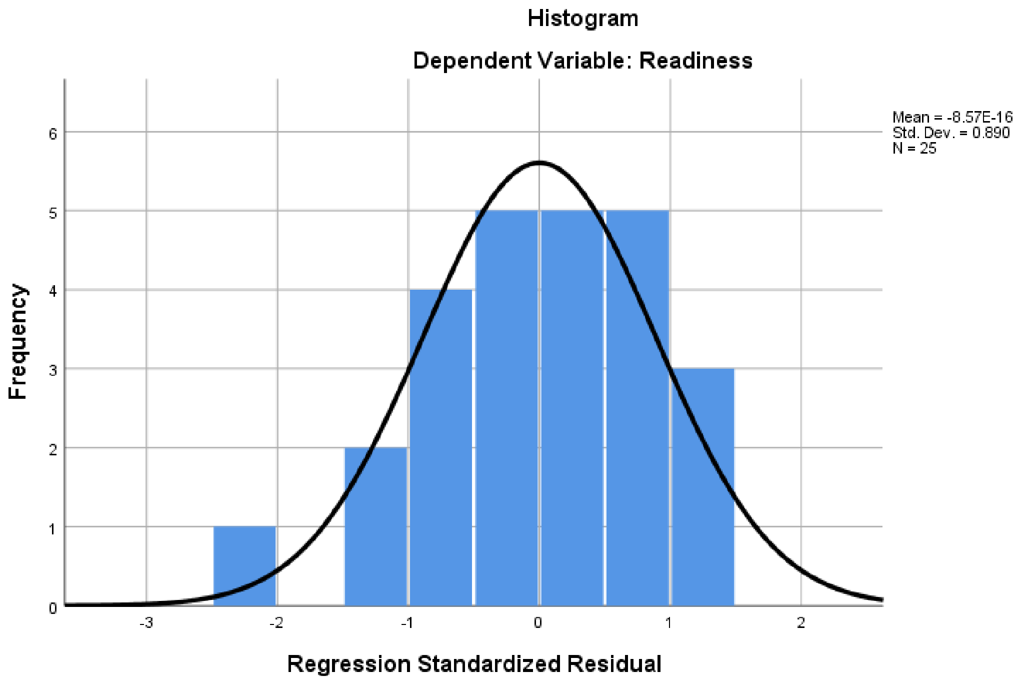


	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	GCI
Angola	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Benin	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Botswana	🟢	🟢	🟡	🟢	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🟡
Burkina Faso	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Burundi	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Cameroon	🟡	🟡	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Cape Verde	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Central African Republic	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Chad	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Congo	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Cote d'Ivoire	🟡	🟢	🟢	🟢	🔴	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟢	🟡	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🟡	🟡
Democratic Republic of the Congo	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Equatorial Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Eritrea	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Ethiopia	🟡	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🟡	🔴	🟡	🟡	🟢	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Gabon	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Gambia	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Ghana	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Guinea-Bissau	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Kenya	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟡	🟡	🟡	🟡	🔴	🟡	🟢	🟡	🟡	🟢	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Lesotho	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🔴	🟡	🔴
Liberia	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟡	🔴	🟡	🔴
Madagascar	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🔴
Malawi	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Mali	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mauritius	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Mozambique	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Namibia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Niger	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟢	🔴
Nigeria	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟡	🟢	🟢	🟡	🟡	🔴	🟡	🔴	🔴	🟢	🟡	🟢	🟢	🟢
Rwanda	🟢	🟢	🔴	🟢	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟡	🟢	🔴	🟢	🔴	🔴	🟢	🟡	🔴	🟡	🟢
Sao Tome and Principe	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Senegal	🟡	🟢	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟡
Seychelles	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sierra Leone	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
South Africa	🟢	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟡	🟡	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🟡
South Sudan	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Swaziland	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Tanzania	🟢	🟡	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🔴	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Togo	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Uganda	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🟢	🟢	🟡	🟢	🔴	🔴	🟢	🟢	🟡
Zambia	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Zimbabwe	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

Appendix IIIII: Regression

Correlations							
		Readiness	Human Resource	Infrastructure	Organization	Environment	Culture
Pearson Correlation	Readiness	1.000	.430	.172	.062	.455	.026
	Human Resource	.430	1.000	.761	.719	.818	.663
	Infrastructure	.172	.761	1.000	.839	.837	.783
	Organization	.062	.719	.839	1.000	.722	.847
	Environment	.455	.818	.837	.722	1.000	.637
	Culture	.026	.663	.783	.847	.637	1.000
Sig. (1-tailed)	Readiness	.	.016	.205	.383	.011	.450
	Human Resource	.016	.	.000	.000	.000	.000
	Infrastructure	.205	.000	.	.000	.000	.000
	Organization	.383	.000	.000	.	.000	.000
	Environment	.011	.000	.000	.000	.	.000
	Culture	.450	.000	.000	.000	.000	.
N	Readiness	25	25	25	25	25	25
	Human Resource	25	25	25	25	25	25
	Infrastructure	25	25	25	25	25	25
	Organization	25	25	25	25	25	25
	Environment	25	25	25	25	25	25
	Culture	25	25	25	25	25	25

Residuals Statistics[a]					
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.9807	4.6791	3.8560	.48858	25
Residual	-1.37394	.76961	.00000	.53513	25
Std. Predicted Value	-3.838	1.685	.000	1.000	25
Std. Residual	-2.284	1.280	.000	.890	25
a. Dependent Variable: Readiness					


Histogram
Dependent Variable: Readiness
Mean = -8.57E-16
Std. Dev. = 0.890
N = 25
Frequency
0
1
2
3
4
5
6
-3
-2
-1
0
1
2
Regression Standardized Residual