ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

CYBER SECURITY PRACTICES AND CHALLENGES AT SELECTED CRITICAL INFRASTRUCTURES IN ETHIOPIA: TOWARDS TAILORING CYBER SECURITY FRAMEWORK

By

TEWODROS GETANEH

JUNE, 2018
ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

CYBER SECURITY PRACTICES AND CHALLENGES AT SELECTED CRITICAL INFRASTRUCTURES IN ETHIOPIA: TOWARDS TAILORING CYBER SECURITY FRAMEWORK

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By: TEWODROS GETANEH

Advisor: Tebebe Beshah (PhD)

JUNE, 2018

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

CYBER SECURITY PRACTICES AND CHALLENGES AT SELECTED CRITICAL INFRASTRUCTURES IN ETHIOPIA: TOWARDS TAILORING CYBER SECURITY FRAMEWORK

By: Tewodros Getaneh

Name and signature of Members of the Examining Board

Tebebe Beshah (PhD) Advisor	_____ Signature	_____ Date
Lemma Lenssa (PhD) Examiner	_____ Signature	_____ Date
Dereje Teferi (PhD) Examiner	_____ Signature	_____ Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that the thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Tewodros Getaneh

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Tebebe Beshah (PhD)

Dedication

This work is dedicated to my beloved sister Eleni Getaneh.

Acknowledgements

I would like to thank my research advisor Dr. Tebebe Beshah for his extrovert guidance and support. He has shown me the right path of research and encouraged me to move forward throughout the study.

I would also like to extend my sincere gratitude to Dr. Andualem Admassie , CEO of Ethio Telecom, for his assistance in time of Data collection.

I am thankful to Ato Mekonnen Tesfaye, ICT Security Head of Ethiopian Electric Utility for his valuable comments and assistance in time of data collection and review of the tailored framework. Your positive attitude towards the research, heartily assistance and encouragement was my energy to move forward throughout this research.

I would like to thank Ato FikreSilase Wosen, an ICT Technician at Ethiopian Electric Utility, for his un - reserved cooperation and assistance throughout this research. My heartfelt thanks goes Ato Yeman Gebre Hiwot of Ethio Telecom and to the whole IT security and Network Security staff at Ethio Telecom. This work was not possible without your support and cooperation.

This study would not have been possible without the help of INSA's Staff for their cooperation and valuable comments. Last but not least I would like to thank my friend Ato Muluken Belete who encourages me to pursue cyber security and for his valuable assistance in evaluating the tailored framework. My heartfelt thanks goes to Mr. Lee Sung Hoon, Director of World Together Ethiopia, for his assistance and positive cooperation.

Table of Contents

List of Tables

List of Graphs

List of Figures

List of Acronyms

BYOD	Bring Your Own Devices
BYOA	Bring Your Own Applications
CERT	Computer Emergency and Response Unit
CIs	Critical Infrastructures
CMSCRS	Critical Mass Cyber Security Requirement Standard
CSF	Cybersecurity Framework
CSFs	Cybersecurity Frameworks
CIO	Chief Information Officer
CSUs	Cyber Security Units
DDoS:	Distributed Denial of Service
DoS:	Denial of Service
GCA:	Global Cybersecurity Agenda
GCI:	Global Cybersecurity Index
ICT:	Information Communication Technology
INSA:	Information Network Security Agency
IoTs:	Internet of Things
IS:	Information System
ISS:	Information Systems Security
IT:	Information technology
NIST:	National Institute of Standards and Technology
UNCTAD:	United Nations Conference on Trade and Development

Abstract

Cyber security is the activity of protecting information and information systems (networks, computers, data centers and applications) with appropriate procedural and technological security measures (Tonge, Kasture and Chaudhari, 2013, p.1). Cyber security threats and breaches are increasing from year to year. A Cyber security breach has the potential to disrupt the proper functioning of nation states. It affects the reputation of organization and erodes customers trust. Cyber security breaches at critical infrastructures can affect the existence of a nation and can disrupt the social, economic and political realm of governments. Critical infrastructures mean any infrastructure vulnerable to information communication network security threats having considerable impact to the social, economic, or political interest of the country.

The purpose of this study is to examine the practices and challenges of cyber security at three selected critical infrastructures in Ethiopia. These critical infrastructures are Ethiopian Electric Power, Ethiopian Electric Utility, and Ethio Telecom. In this study attempts were made to tailor cyber security framework based on the challenges of cyber security, INSA's Critical Mass Cyber Security Requirement Standard Version 1.0 and NIST Framework to improve critical infrastructures cyber security version 1.1.

The study is based on International Telecommunication Union's /ITU/ Cyber Security Agenda three pillars Legal, technical and Capability Building. The core processes of NIST framework, Identify, Detect, Prevent, Respond and Recover functions are used as technical sub pillars.

This research used both qualitative and quantitative research approaches. Questionnaires and Interviews are used as data collection instruments. The questionnaire is adopted and modified from International Telecommunication Union's Global Cyber Security Index of 2017 and MIT Technology Review Customs Research of 2016.

The study subjects are the total population of IT/ICT security or cyber security unit of the selected critical infrastructures. The total of 75 questionnaires were distributed with a response rate of 84%. Interviews were conducted to grasp the processes, challenges and to evaluate the tailored cyber security framework.

Descriptive data analysis techniques are used in SPSS version 23 on the data collected using questionnaire. The survey indicated that the top rated cyber security challenges are lack of in-house expertise (66.7%), inadequate enabling technology and difficulty in locating the right security alert (with equal percentile of 61.9%), and evasion of existing preventive security controls (60.3%).The survey also indicated that attack via Email (74.4%), attacks via mobile computing (68.3%), and attacks via social media (63.5%) are on growing trend of cyber security.

Moreover this research indicated that the selected critical infrastructures are inadequately prepared to detect, prevent, and respond to cyber threats and breaches. It is not only the technical issues that show a grim picture but the executives or the top branch management are not adequately prepared to prevent and respond to cyber threats and breaches.

Based on the findings, attempts were made to propose a tailored cyber security framework based on INSA's Critical Mass Cyber Security Requirement Standard Version 1.0 and NIST's Framework for improving critical infrastructures cyber security version 1.1.

Furthermore, in order to tailor the cyber security framework, this research conducted extensive literature review on cyber security framework development. Additionally attempts were made to follow design science guidelines in the process of tailoring the cyber security framework. The tailored cyber security framework is further evaluated for its coverage, suitability, comprehensiveness, clarity, completeness and applicability by using questionnaire and interview.

Finally conclusions and recommendations were made based on the findings and analysis.

Key words: Cyber security, Security, Cyber Security challenges, Framework

CHAPTER ONE

1. Introduction

1.1 Background

The birth of the internet as a project of ARPA net in US ministry of defense grew to a global network and paved the way to globalization. The internet, which is a network of networks, is a global IT infrastructure which transforms the global social, economic and political environment. Desisa and Beshah(2014) stated that ever since the birth of the Internet, people have been using it more and more for accomplishing their daily tasks (p.1). The Global Cyber security Index/GCI/ of 2017 report affirmed that the information and communication technologies /ICT/ networks, devices and services are increasingly critical for day-to-day life (Global Cyber security Index, 2017, p.1). Accordingly Munk (2015) stated that the increased dependency on cyber-space is visible in all public-private sectors and governmental operations, as well as communications between groups and individuals (p.7). In further strengthening this, Global Cyber security Index of 2017 report stated the global community is increasingly embracing ICTs as key enabler for social and economic development (Global Cyber security Index, 2017, p.iii).

Computer networks specifically the internet affects nearly every aspect of human life. Munk (2015) stated that the highly decentralized and increasingly complex internet is anchored in every aspect of public and private computing (p.12). The same author further stated that for all its user friendly attraction, and promises, the internet is effectively a ‘series of tubes’ and ‘cloud’ that connect everything from facebook accounts, to bank accounts, to aspects of critical governmental and private infrastructure (p.12). Computer networks enable financial institutions to operate at high level of efficiency. Private institutions highly depend on information technology for running their daily business. Governments tab in to the internet and computer networks for efficient data processing, storage and dissemination. Bogale (2016) in strengthening this concept stated that in many organizations, information technology (IT) has become crucial in the support, sustainability and growth of the business (p.25).

This phenomenon gives rise to a cyberspace. Even if cyberspace and its services transform most aspects of today's business and individual communication, there is a high risk of danger lurking around the corner. Munk (2015) summarizes this as cyberspace creates a virtual world that enables criminal acts, where the criminal activity takes place within or by utilizing networks of electronic communication such as the internet (p.12).So what is cyber crime constitutes of? Euro Just's Annual Report 2011 states that:

> *The term "cyber crime" encompasses two types of criminal activity: the use of the internet to commit "traditional" crimes such as fraud, forgery, publication of sexual abuse material, etc., and the use of electronic means to disrupts or completely immobilize information systems.(As cited in Munk,2015, p.48)*

Cyber criminals target individuals, companies and governments for personal or economic gains. Wu and Irwin (2013) stated that although the targets of cyber attacks vary widely, they are primarily focused on money, intellectual property and of course sabotage (p.29). Cyber attacks use technical innovations like bugs, warms, virus and denial of service. State-of-the-art report (2009) stated that the rapid growth of connections, processing, bandwidth, users, and global dependence on the internet has greatly increased vulnerability of information technology infrastructure to increasingly sophisticated and motivated attacks (As cited in Munk,2015, p.19).Therefore there is high need to secure cyberspace.

The process of safeguarding cyberspace is the main concern of Cyber security. So what is Cyber security? Tonge, Kasture and Chaudhari(2013) define Cyber security as the activity of protecting information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures (p.1).

Even if Cyber security is one counter measure to cyberspace crime, it is not possible to ensure a total security. Munk (2015) stated that the reality of cyberspace in the 21st century is that nothing is secure (p.13).This is because there is a direct cause-effect principle between growth of ICTs and their illicit and malicious use (Global Cyber security Index, 2017, p.1).Munk (2015) further stated that what now constitutes a Cyber security risk has evolved from a single matter of protecting a computer network from outside intrusion or physical access, to protecting entire

nations, its citizens and their most sensitive information (p.12). Cyber security is, therefore the main concern of developed and developing nations.

Bruce S. Schaeffe et al. (2009) stated that: Cyber-crime is on the rise everywhere. On average, there has been a reported cyber-security event every single day since 2006 (p.1). Due to this, US President Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the twenty-first century will depend on cyber security" (As cited in Hailu, 2015, p.2).

In developed countries, it is obvious that most of the sectors of the economy highly depend on cyber space for most of their daily operations. Even if all the sectors of a nation are significant for the proper functioning of government and a society, selected sectors are considered to be critical infrastructures. USA Patriot act and critical infrastructure act of 2001 (42 u.s.c 5195 c(e)) define:

> *Critical infrastructure as means systems and assets, whether physical or virtual to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

Based on this definition of critical infrastructure, US department of home land security and presidential policy directive PPD – 21 identified 16 critical infrastructure sectors. Some of the critical infrastructures are chemical sector , communications sector , critical manufacturing sector , dams sectors , defense industrial base sector , emergency services sector , energy sector ,financial service sector ,government facilities sector , transportation systems sector and Nuclear Reactors, materials and waste sector.

Federal Democratic Republic of Ethiopia Council of Ministers Regulations for the establishment of the Information Network Security Agency /INSA/ Regulation No. 130/2006 defines critical infrastructures as:

> *"Critical Infrastructures" means any infrastructure vulnerable to information communication network security threats having considerable impact to the social, economic or political interest of the country.*

Even if there are no clearly identified critical infrastructure sectors in Ethiopian context, this research uses the American Experience to identify and select critical infrastructure for this Cybersecuirty study.

Based on the above definitions of critical infrastructure, this research uses a case study of Ethiopian Electric Power/EEP/, Ethiopian Electric Utility /EEU/, and Ethio Telecom. EEP & EEU are the only government organizations that generate power and distribute to its customers. Ethio Telecom is the only Telephone and Internet Service Provider /ISP/ owned by the government. These three infrastructures should be protected from any Cyber security breach and as such are taken as cases for this research and as such taken as cases for this research.

Ethiopia like any other nation is not immune from cyber attack. The United Nations Conference on Trade and Development (UNCTAD) indicated that developing countries have become staging grounds for attacks by cyber criminals due to the greater prevalence of unprotected systems (As cited in Hailu, 2015, p.6) .There are several instances of cyber attacks. In order to combat cyber attacks, the Ethiopian government enacted legal framework i.e Telecom Fraud offence proclamation761/2012 and goes even further in establishing INSA /information Network Security Agency/ in 2006 with Council of Ministers Regulations No. 130/2006.

There is also global initiative in cyber security by International Telecommunication Union/ITU/ in collaboration with other organizations. One of this initiative is Global Cyber Security Index /GCI/. International Telecommunication Union /ITU/ with 193 member states measures the commitment of ITU Member States towards cyber security in order to drive further efforts in the adoption and integration of cyber security on a global scale (Global Cyber security Index, 2017, p.iii). In order to measure the commitments of Member States in cyber security , ITU developed a Global Cyber security Index / GCI / based on Global Cyber security Agenda's / GCA/ five pillars namely Legal , Technical ,organizational , capacity building and cooperation.

According to Global Cyber security Index report of 2017, Ethiopia is at initiating stage at Global Cyber Security Index score and ranks 14th and 98th in Africa and in the world respectively (Global Cyber security Index, 2017, p.13, 51). The GCI includes 25 indicators and 157 binary questions. Based on the data collected and analyzed from 193 member states, GCI prepared score card for each region.

The African region score card shows that Africa as a region is categorized as low in the three GCA pillars namely technical, organizational and capacity building. Moreover GCI 2017 African region score card shows that Ethiopia is specifically in low category in legal and technical pillars. The details of the score show that cyber security legislation and training, standards for organizations and professionals, sectorial CERT and child on line protections should be given due emphasis for improvement (Global Cyber security Index, 2017, p.9, 22).

However the GCI 2017 report did not provide sector specific recommendation for each country. Therefore this research studies Cybersecuirty at critical infrastructures based on the three pillars of GCA, i.e. Legal, Technical, Capability Building, in order to recommend solutions for current and future challenges of Cyber security and to propose a tailored Cyber security framework based on NIST framework for improving critical infrastructures Cyber security version 1.1 and INSA's Critical Mass Cyber Security Requirement Standard Version 1.0..

The diagram on figure 1.1 shows the five Global Cyber security Agenda's /GCA/ pillars and sub pillars.

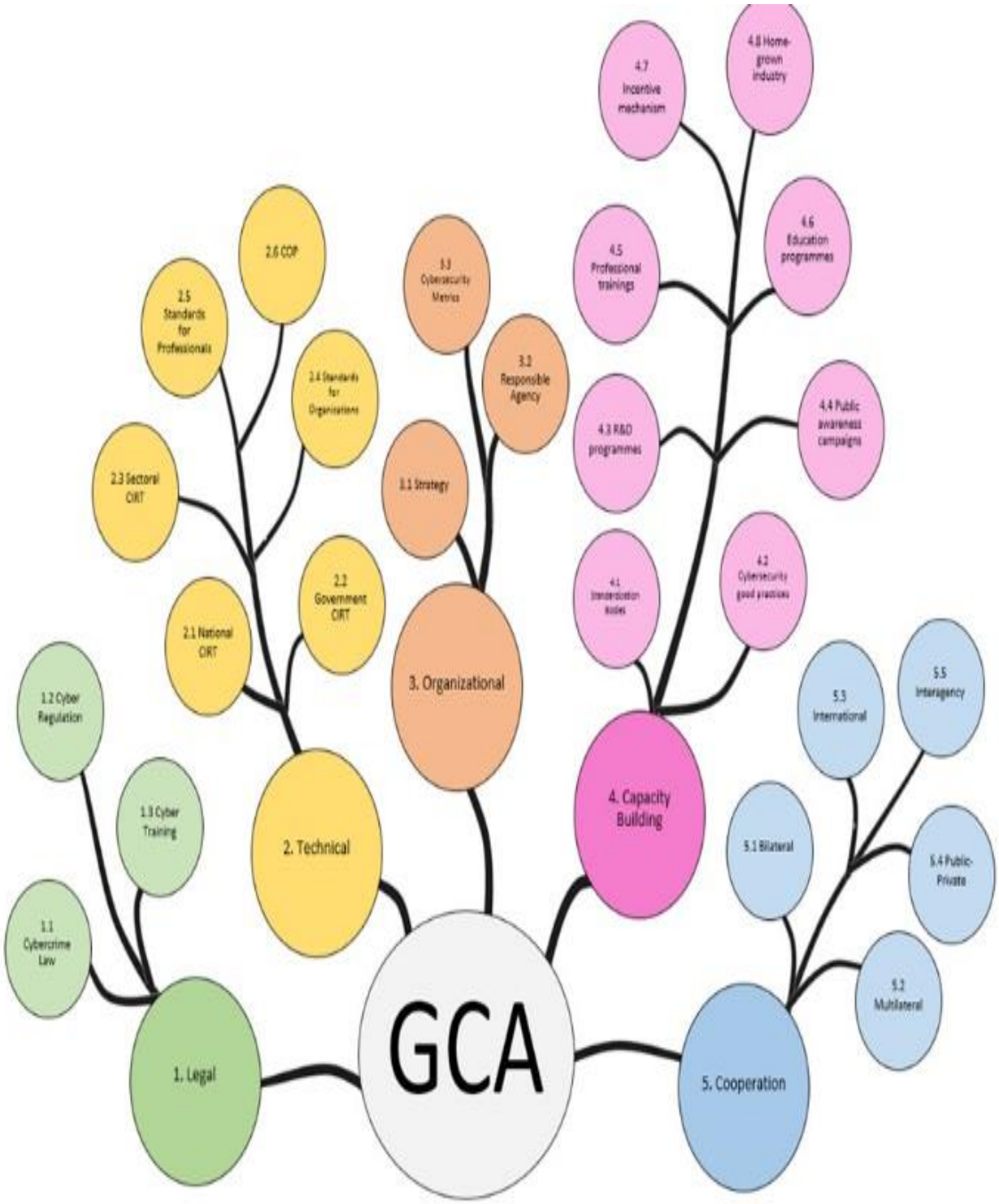


Figure 1.1: Global Cyber security Agenda / GCA / Tree Structure Illustrating all Pillars (Simplified)

(Global Cyber security Index, 2017, p. 6)

1.2 Statement of the Problem

Ethiopia, even if it has started to use and spread network technologies and the internet recently, the success and even existence depends on this technology. Even if the penetration of the internet in Ethiopia is insignificant when compared with developed countries, the opportunities and the challenges of this technology is relatively similar. The main challenge of computer network, the internet, is security. Alabady (2009) define Network security as a process by which digital information assets are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability (p.1). This process of securing information in cyberspace is referred as Cyber security.

Although tremendous amount of effort and money is invested in research in areas of Cyber security, Ethiopia is far from safe guarding its cyberspace. There are several instances of cyber breach. US based off price retailer TJX announced on January 17, 2007 where 130 million credit and debit cards data of its customers were compromised. This security breach was the result of coordinated and networked hackers , stretched from US to Europe led by Albert Gonzalez with ironic title of their operation as get rich or die trying (salim,2014,pp.65-91). BBC news reported that US based credit report giant Equifax announced on September 8, 2017 that 143 million of its customer's data was compromised in a Cyber security breach. Similarly cyber security breach at yahoo exposed one billion records. Moreover 412 million and 200 million records were exposed in cyber security breach from friend finder network and of US voters respectively. Furthermore CNN news reported on October 11, 2017 that state sponsored cyber security breach by North Korea hackers stole US-South Korea war plans and 235 Giga bytes of military data.

Even though there is no well compiled report of cyber crime and threats in Ethiopia like developed countries, there are some instances. Muluneh (2017) stated that due to lack of studies in the area of Information System Security /ISS/, it is difficult to know the exact statistical figure with respect to financial losses of the incidents. The same author further stated some of the security breaches in his doctoral dissertation. Muluneh (2017) stated the incident of security breach at Ethiopian Revenue and Custom Authority by junior database administrator which cost the organization 13,000,000 Birr. Moreover the author further states the security breach at

Ethiopia air lines related to sheba miles by its own Employees. Furthermore there are instances of cyber attack every year according to yearly report of INSA.

Therefore, cyber crime is real, immediate and tangible danger for businesses and government of Ethiopia. Due to this reason the Ethiopian government enacted a legal framework, i.e Telecom Fraud offence proclamation761/2012. The Ethiopian government even goes further in formulating Cyber security affiliated information security policy /ISP/. This information security policy targets on effective use of IT infrastructure in transforming the social, economic and political sphere of Ethiopia. Moreover, considering the threats and possibility of imminent danger associated with Cyber security, the government of Ethiopia established Information Network Security Agency /INSA/ in 2006 by minister of council proclamations number 130/2006. INSA is established in order to ensure safe-heaven for businesses and the government in cyberspace. However, the safe heaven on cyberspace is real challenge for INSA.

In academics, several researches were conducted in aspects of security. These researches mainly focused on insider threats, information security policy and IT audit. Negussie (2015) in his thesis studied the practices, challenges and prospects of information policy in Ethiopian banking industry. Amare(2015) performs organizational specific security related research on assessment of insider threat in Ethiopian Banking Industry. Moreover Bogale (2016) in his doctoral dissertation studied IT Auditing and IT governance. In this research the researcher examines the factors to be considered in IT Auditing and the influence of IT governance and organizational performance. Furthermore Muluneh(2017) studied employee's information security policy violation and rational choice theory in Ethiopian context. Desisa and Beshah(2014) studied and developed Internet Banking Security Framework for Ethiopian Banking Industry. Furthermore there are researches performed in aspects of security like Gebrehawariat(2017) on assessment of the effectiveness of card banking security, Haddish(2013) and Adane (2011) fraud detection by using data mining technologies for Ethiopian telecom and African insurance share company respectively. As stated above the previous researches focus on specific aspect of security like fraud detection, insider threat, information systems security policy and IT auditing. Moreover the researches were focused on specific organizations like banks and insurance companies. These

researches contribute a great deal in building knowledge on aspects of security and as well provide a remedy for the organizations.

There is a wide area of Cyber security issues that is not researched or studied at a national level. One of the global initiatives in cyber security, Global Cyber security Index/GCI/ of 2017 clearly identified that Ethiopia needs to enhance legal, technical and Capability Building measures of the Global cyber security pillars. Moreover the same index clearly stated that Ethiopia needs to work towards enhancing sector specific CERT, standards for organization and professionals and child online protection.

This study is proposed in order to study and identify the challenges and recommend solutions for current and potential challenges in ensuring safe cyberspace based on GCA three pillars of the five namely Legal, Technical and Capability building. To secure critical infrastructure there is a need for appropriate framework for organizations based on their context. NIST framework (2017) stated that the framework is not a one-size-fit all approach to managing Cybersecurity risks for critical infrastructure (p.6). Similarly Critical Mass Cyber Security Requirement Standard Version 1.0 which was issued in 2016 by Information Network Security Agency of Ethiopia stated that cyber security management system and risks should take its content of 80% from national and sectoral common risk profile and 20% based on its own context (CMCSRS version 1.0, 2016, p.36, p.63). It also stated that organizations should also identify 80-20 in each area and focus on the 20% based on 80-20 rule (Pareto Principle) (CMCSRS version 1.0,2016,p.22).

Therefore this study attempt has been made to tailor an existing cyber security framework for selected infrastructures which enables these organizations to be more efficient in identifying cyber security threats and vulnerabilities and to recommend an efficient process to respond and to recover from cyber security breach.

1.3 Research Questions

This research answers three questions. These questions are:

I. What are the challenges faced in ensuring safe cyberspace at the selected critical infrastructures in Ethiopia?
II. What processes and practices are implemented at selected critical infrastructures in Ethiopia to ensure Cyber security?
III. What would be an appropriate Cyber security framework for the selected critical infrastructures?

1.4 General objective of the Research

This research investigates the practices and challenges of cyber security to adapt, modify and tailor a cyber security framework for the selected critical infrastructures in Ethiopia.

1.5 Specific objectives of the Research

The specific objectives of this research are:

- To pin point the challenges of cyber security at the selected critical infrastructures.
- To identify the existing processes and practices of cyber security at selected critical infrastructures.
- To recommend solutions for existing challenges of cyber security at selected critical infrastructures.
- To recommend enhanced cyber security process at selected critical infrastructures.
- To tailor a cyber security framework for selected critical infrastructures.

1.6 Scope and Limitations of the Research

This research only covers three selected critical infrastructures practices and challenges of cyber security in Ethiopia. The research only considers critical infrastructures located in Addis Ababa. Due to the cost and time constrains, it does not consider all the critical infrastructures for the study.

This research targets to identify practices and challenges of cyber security at critical infrastructures from IT security or security compliance units or cyber security units' staff. Cyber security challenges can be studied from end users perspective. However due to time and finance limitations, end users are excluded from the study.

This research Examines Cyber security practices and challenges at critical infrastructures in Ethiopia based on global cyber security three pillars namely Legal, Technical and Capability building. It excludes the other two pillars, organization and cooperation, due to financial and time limitation.

1.7 Significance of the Research

This research contributes to existing efforts in cyber security by identifying the challenges at selected three critical infrastructures in Ethiopia. Moreover it assists Information Network Security Agency /INSA/ in developing sector specific Cybersecuirty framework for the other government sectors in Ethiopia. Additionally this research provides a solution for Cyber security problems faced by each critical infrastructure. The Cyber security unit of each critical infrastructure can use this research and further engage in research in other areas of Cyber security.

1.8 organization of the Thesis

This research contains six chapters. The present chapter, chapter one, discusses an introduction, statement of the problem, research questions, general and specific objectives, scope and limitations, and significance of the research. The second chapter, literature review and related works, discusses the conceptual framework of the research and review of related works. In this chapter Cyber security threat actors and methods, national and global Cyber security initiatives are discussed. Moreover this chapter briefly discusses Global Cyber Security Index /GCI/ 2017 pillars and sub pillars, INSA's Critical Mass Cyber Security Requirement Standard/CMCSRS/ Version 1.0 and NIST framework for improving critical infrastructure Cyber security draft version 1.1.

The third chapter, research methodology, discusses the general methodology this research follows. Moreover in this chapter, the research pillars and sub pillars, data collection instruments and data analysis methods are presented. Data presentation, analysis and discussion are presented in chapter four. The next chapter, chapter five, discuses the tailored Cyber security framework based on NIST framework for improving critical infrastructure Cyber security draft version 1.1

and INSA's Critical Mass Cyber Security Requirement Standard /CMCSRS/ Version 1.0. Finally the last chapter, chapter six, discusses the conclusion, recommendation and future area of research in Cyber security.

CHAPTER TWO

2. Literature Review and Related Works

2.1 Overview

The objective of this chapter is to build conceptual framework for this study and to discuss related works on aspect of cyber security. This chapter begins by describing and differentiating three related phrases and concepts; Computer Security, Information Security and Cyber security. This portion also discusses the Cyber security threat actors and the known methods used for cyber security breach. Moreover it also discusses the national and global cyber security initiatives. Furthermore as the research studied Cyber security practices and challenges at selected critical infrastructures in Ethiopia based on the ITU's Global Cyber security Agenda's three pillars, it discussed these pillars and their sub pillars. The INSA's Critical Mass Cyber Security Requirement Standard /CMCSRS / version 1.0 is presented. NIST framework for improving critical infrastructure Cyber security version 1.1 is discussed. Finally two related cyber security survey researches are discussed.

2.2 Computer Security, Information Security and Cyber security

Due to the development of technology specifically ICT, the concept of security changes through time. Prior to the existence and developments of computer networks and the internet, the concept of security revolves around military. Munk(2015)stated that the definition of threat and security has changed over years (p.3). This shows that it's not only the definition of security that is altered, but the concept of threat, control and the process of mitigating these threats.

There are at least three related concepts in relation to security. These are computer security, information security and Cyber security. Solms and Niekerk (2013) define computer security, also known as information communication / ICT/ security, is the security of the computers that process and store information (As Cited in Horne, Ahmed and Maynard, 2016, p.4). The same author further stated that the goal of computer security is the confidentiality, integrity, availability, non repudiation, accountability, authenticity and reliability of information resources.

The second concept of security, information security, refers to protecting information and information systems from unauthorized access, use, disclosure, disruption or destruction.

According to Mcumber (1991) and Solms(1998) the goal of information security involves preserving the confidentiality, integrity and availability of business information (As Cited in Horne, Ahmed and Maynard, 2016, p4). Solms (1998) further stress that information security needs to safeguard business continuity and reduce business impairment by constraining the effect of security incidents (As Cited in Horne, Ahmed and Maynard, 2016, p4). The International Telecommunication Union /ITU/ defines cyber security as follows:

> *Cyber security is the collection of tools , policies, security concepts , security safeguards, guidelines, risk management approaches , actions, training , best practices , assurances and technologies that can be used to protect the cyber environment and organization and user's assets. Organizations and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and /or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general objectives comprise the following:*
>
> - *Availability*
> - *Integrity , which may include authenticity and non-repudiation*
> - *Confidentiality (ITU,2008)(As Cited By Solms and Niekerk ,2013,p.2)*

The same authors stated that Cyber security is different from information security. They further stated that although they are very different, the term Cyber security seems to be used interchangeably with the term information security in academic literatures. The same authors stated that Cyber security transcend the boundaries of information security to include the defense of information and also people (As Cited in Horne, Ahmed and Maynard, 2016, p4). The same author further stated that the goal and general security objectives of cyber security are availability, integrity and confidentiality of an organization's assets including networks, infrastructure, information and personnel (As Cited in Horne, Ahmed and Maynard, 2016, p4). The ITU – T recommendation X.805 stipulates 8 cyber security dimensions : namely

authorization , authentication , availability , communication security , confidentiality , integrity , non – repudiation and privacy (As cited in Boateng ,2013, p.49). Even if these terms are related mainly in their goal, Cyber security is broad concept than information security and computer security. The following diagram (figure 2.1) shows the relationships between information and communication security, information security and cyber security.

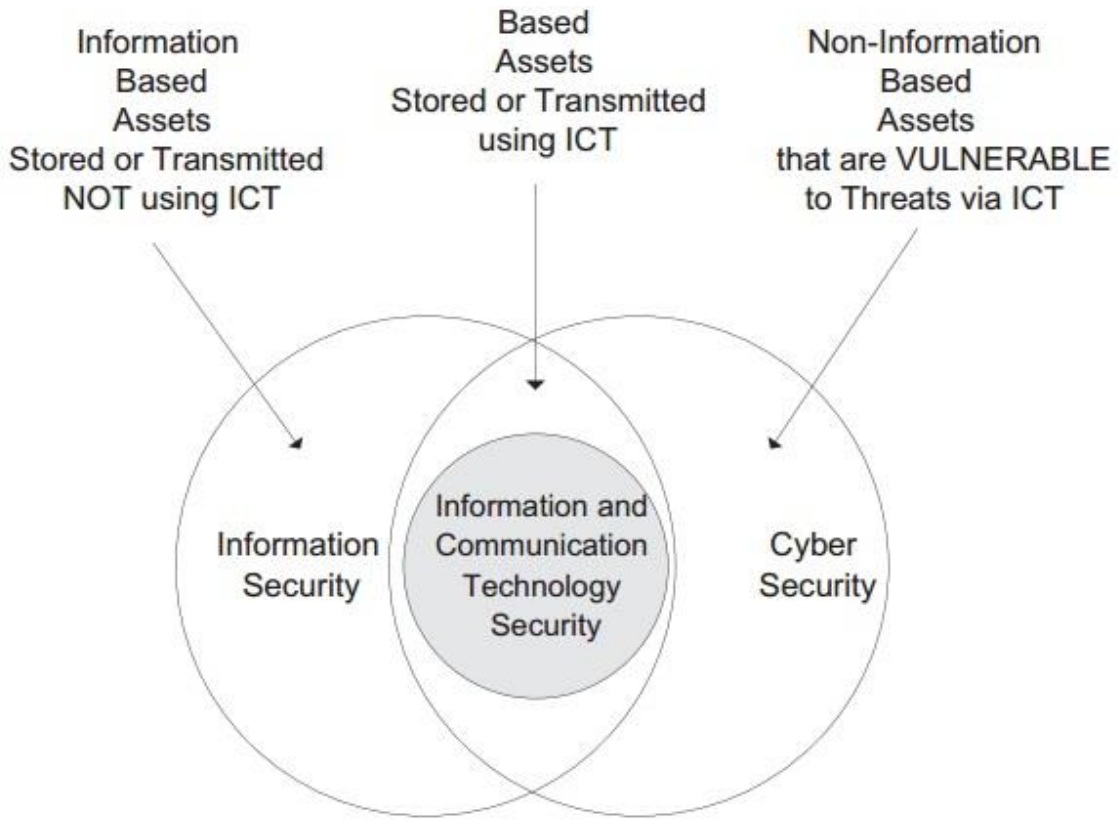


Figure 2.1 The relationships between information and communication security, information security and cyber security. Source (*Solms and Niekerk ,2013,p.7*)

2.3 Cyber Security Threat Actors

Cyber security breach of any kind can be perpetuated intentionally or unintentionally. There are several threat actors namely Hackers, Hactivism , State and State affiliated actors, and company insiders / malicious users /.

Sahare, Naik and Khandey (2014) explain hacking is an activity in which , a person exploit the weakness in a system for self-profit or gratification (p. 1) . This activity is done by Hackers.

They are also called crackers, intruders or attackers. Their motivation for hacking is diverse. The same authors further stated that some hackers do it for fun, some do it for profit or some simply do it to disrupt your operations and perhaps gain some recognition. Hacking can be classified in three different categories, according to the shades or colors of the "Hat". The word Hat has its origin from old western movies where the color of hero's cap was 'white' and the villains' cap was 'black'. It may also be said that the lighter the color, the less is the intention to harm (Sahare, Naik and Khandey ,2014,p.1).

Based on these premises, the authors categorized hackers in to three groups namely Black Hat Hackers, White Hat Hackers and Gray Hat Hackers. White hat hackers are authorized and paid by the companies, with good intents and moral standing. They are also known as IT technicians. Some companies pay IT professionals to attempt to hack their own servers and computers to test their security. They break security to test their own security system. The white hat hackers are also called Ethical hackers. However, the intention of Black hat hacker is to harm the computer systems and network. These categories of hackers break the security and intrude into the network to harm and destroy data in order to make the network unusable. Moreover they deface the websites, steal the data, and breach the security. As like inheritance, some or all properties of the base class or classes are inherited by the derived class, similarly a gray hat hacker inherits the properties of both black hat and white hat hackers. These hackers may offer the remedy. They are well aware of what is right and what is wrong but sometimes act in a negative direction (Sahare, Naik andKhandey ,2014,p.3) .

Kosina(2012) describe Hacktivism is a neologism of unknown origins blending the words "hacking" and "activism". Hacktivisms are individuals who engaged in hacking activities, including trying to gain unauthorized access to computers or networks, in order to further social or political ends (P.22). Hacktivism falls in to the grey area between politics and crime, most closely resembling what is traditionally understood as subversion-"the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order" (Kosina, 2012, P.22).

In addition to hackers and hacktivism , cybercrime and cyber breach is also perpetuated by organized crime groups and state and state affiliated proxies. Broadhurst et al.(2014) stated that today we find that numerous governments / or their proxies / are using internet technologies to commit crime. The same authors further stated that allegations that Russia has executed or encouraged distributed denial of service attacks , and that Chinese authorities are engaged in wide spread economic and industrial espionage, have been matched by the disclosures of Edward Snowden that united states governments has engaged in massive programs of cyber-surveillance. Moreover governments , law enforcements agencies , academic researchers , and the Cyber security industry, speculate that 'conventional' organized crime groups have become increasingly involved in digital crime (Broadhurst et al. ,2014,p.3).Mc Guire's(2012) review , based on large sample of known cases , found that up to 80% of cyber crime could be the result of some form of organized activity (As citedBroadhurst et al. ,2014,p.3). Broadhurst et al.(2014) stated that in recent years , insurgents and extremist groups have used internet technology as an instrument of theft in order to enhance their resource base. Sipress(2004) stated that Imam Samudra , convicted architect of the 2002 Bali bombing , reportedly called up on his followers to commit credit card fraud in order to finance militant activities(As cited Broadhurst et al. ,2014,p.3). It is also a known fact that insurgents and extremist groups used the internet as a medium to spread their propaganda and recruit new members.

Broadhurst et al.(2014) stated some of the motivations behind hacking by citing instance for each case. Some of the motivations for hacking as stated by the authors are:

- Guided by ideology and the desire to challenge powerful interest.
- A desire to demonstrate technical proficiency.
- Rebelling against the prevailing system of intellectual property.
- Voyeurism re-enforced by obsessive / compulsive behavior.
- Retaliation by disgruntled former employee and
- For financial benefit (Broadhurst et al. ,2014,p.8-10) .

The other groups of security threats are malicious insiders. The former US secretary of defense and director of CIA Leon Panetta sum up a grim new reality caused by malicious hackers as " malicious hackers are threatening our basic infrastructure, and a 'Cyber Katrina' or even a

'Cyber 911' appear to be a matter of time"(As cited by Kosina,2012,P.9). According to Symantec (2009) report on Anatomy of a data breach malicious insiders constitutes drivers for a growing segment of data breaches, and a proportionately greater segment of the cost to business associated with those breaches (p.8). The same study further stated that the Ponemon study found that data breaches involving negligence cost $199 per record; where as those cause by malicious acts cost $255 per record. This shows that the cost of data breach caused by malicious insiders is far greater than the cost caused by negligence. According to semantic report of 2009 company employees who inadvertently violate data security policies continue to represent the largest population of data breaches (p5). Verizon report stated that 67% of the breaches in 2008 were aided by "significant errors" on the part of well-meaning insiders. Moreover in 2008 survey of 43 organizations that had experienced a data breach , the Ponemon institute found that over 88% of all cases involved incident from inside negligence(As cited in White paper: enterprise security Symantec,2008,p.5). The same report further stated that analysis of breaches caused by well-meaning insiders yields five main types:

- Data exposed on servers and desktops: perhaps the most common type of data breach occurs when well-meaning insiders, unaware of cooperate data security policies, store, send or copy sensitive information unencrypted.
- Lost or stolen labtops: the 2008 Ponemon institute study found that lost labtops were top cause of data breaches representing 35% of organizations polled. It further stated that a typical large enterprise, missing laptops are a weekly occurrence.
- E-mail, web mail and removable devices: risk assessment performed by Symantec for prospective customers show that on average approximately one in 400 email messages contains unencrypted confidential data. Such network transmissions create significant loss.
- Third party data loss incident, and
- Business processes automate the spread of sensitive data (White paper: enterprise security Symantec, 2008, p.6).

The report of Symantec (2009) stated that the breach caused by insiders with the intent to steal fall in to four groups:

- White collar crime: These groups of company insiders abuse their privilege access to information for the purpose of personal gain.

- Terminated employees: A recent study of the effects of employee terminations on data security revealed that 59% of ex-employees took company data, including customers' lists and employee records.
- Employee's who breach security for the purpose of career building with company data and
- Employee's who breach security for the purpose of industrial espionage (p.9).

2.4 Methods of Cyber Attack

Cyber attack takes different forms based on the objective of the attacker. Some of the known methods employed by attackers are Social Engineering, Denial-of-Service /DoS/, Distributed – Denial-of-Service /DDoS /, Website Defacement and Malicious Code. Each of these cyber attack methods are discussed below.

2.4.1 Social Engineering

Conteh and Schimick(2016) define social engineering , also known as human hacking , is the art of tricking employees and customers in to disclosing their credentials and then using them to access to networks or accounts (p. 1). The same authors further stated that Social engineering as a tactic deploys techniques to gain access to private and confidential information by exploiting flaws in human logic known as cognitive biases (p. 2).This scheme uses human inner behavior, curiosity and deception. The same authors further stated that it is a hacker's tricky use of deception or manipulation of people's tendency to trust, be corporative, or simply follow their desire to explore and be curious. In other words, an attacker engages social engineering as a tactic to use insiders and information to circumvent computer security solutions through deceit (Conteh and Schimick, 2016 p.2). Whatever technological progresses are made in preventing cyber security breach, one of the factors that cannot be avoided is weakness in human link. Due to this Conteh and Schimick (2016) stated that while security measures aim at improving information system security, human factors represent a weak link which is exploited during a social engineering attack (p.2).

Bisson (2015) notes that social engineering encompasses a broad spectrum of malicious activity and identifies five of the most common types of social engineering attack victims which includes

phishing, pre-texting, Baiting, Quid pro qou and Tailgating. (As cited By Conteh and Schimick, 2016, p.2).

Conteh and Schimick (2016) describe phishing scams as an attempt to obtain personal information such as names, address and other personal identifiable information such as social security numbers. Phishing scams may embed links to redirect users to suspicious websites that appear legitimate. It also uses an e-mail service for attack. This social engineering type, phishing scams create a sense of urgency to manipulate users to act in a manner that challenges good judgment (p.4).

The same authors describe pre-texting, which is the second type of social engineering, is driven by a fabrication scenario attempting to confirm and steal personal information from a target. This method requires the attacker to build a credible story that leaves little room to question doubt by target. The strategy is to use fear and urgency while building a sense of trust with a victim to confirm or obtain sought information (p.4). Baiting is similar to phishing attack. Hackers use the lure of promised goods if a user surrenders login credentials to specific site. Quid pro quo which is similar to baiting is where an attacker impersonates information technology representative and offer assistance to victims who may be experiencing technical challenges. The last social engineering attack, in tailgating, the attacker uses tailgating and piggy backing to gain access to restricted areas. This attack exposes those who have an ability to grant or gain access to a restricted area by an attacker who may impersonate delivery personnel or others who may require temporary access (Conteh and Schimick, 2016, p.4).

2.4.2 Denial-of-Service /DoS/

Kosina(2012) define Denial-of-Service /DoS/ attack as an attempt to make an online resource often a website unavailable to its legitimate users(P.16). This attack method is implemented by sending a stream of request for servers. The same author describes this method as DoS attacks work by “flooding” the resource with a large number of requests. The author further explained the effect of this attack as it overwhelms the server, which is no longer responding to all the requests (Kosina, 2012, P.16). Luo, Chang and Chan(2005) stated that Denial-of-Service /DoS/ attacks are among the most detrimental, which affect computer and communication performance

through resource exhaustion in terms of compute cycles, buffers , and communication bandwidth (As Cited By Chee-Wooi Ten, 2010.p.3).

However for this attack, a single computer or limited number of computers will not give the desired result for the attacker. Because it is easy to block the originating source of DoS attack. Due to this, most DoS attacks are Distributed-Denial-of-Service/DDoS/ attacks. Kosina(2012) stated that DDoS attacks can be conducted by having computer users voluntarily join forces to participate in the attack. The author stated that more commonly, DDos attacks are orchestrated using botnet-networks of compromised computers whose users are not even aware that their machines are involved in attack. Malicious software / Malware/ installed on the computer allows a third party ,the actual attacker, to take control of the machine and turn it in to a bot /short for robot/ participating in the DDoS attack (Kosina, 2012, P.17). The same author further stated that Denial-of-Service attacks are among the most wide spread cyber attacks.

2.4.3 Website Defacement

Kosina(2012) describe website defacement as an attack on a website that changes the content of that website. Kosina further stated that the new content reflects the motivation of the attacker / for instance stating his or her political or ideological believes /ridicules the target or both(Kosina, 2012, P.18). The same author further stated that one of the most common methods for website defacements is a technique known as SQL injection which is actually a method of passing commands to a database by entering malicious data in a web form.

2.4.4 Malicious Code

Malicious code is a programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computing system; encompasses Trojan horses, malware, viruses, warms and trapdoors (Dictionary of computing and communications, 2003). These malicious codes are capable of duplicating and transmitting themselves in a computer network. They can also be transmitted from computer system to another computer system using flash disk and from devices of inside users/Bring your own Devices: BYOD/.

2.5 Cyber security in Ethiopia

Ethiopia as developing nation is highly dependent on cyberspace. Most economic sectors depend on information technology and network in order to run their daily task. Recognizing this fact the Ethiopian government in its Critical Mass Cyber security Requirement Standard (2017), from now on referred as CMCSRS, stated that government and non-government organizations in Ethiopia are highly relying on information and communication technology, and information is becoming invaluable economic, political and social asset of the nation and a resource to transform the country (p.7). The government of Ethiopia not only recognizes the benefits of information and information technology communication, but the potential danger lurking around every corner in cyberspace. CMCSRS version 1.0 (2017) stated the need for delicate balance between risk and benefit as the reliance on information systems is increasing the vulnerability of organizations to cyber attacks which are becoming highly complicated, dynamic and destructive. It further stated that it is essential to ensure the security of organizational information systems in order to protect organizations from cyber attacks and to minimize the impact of cyber attack on the country (p.7).

In recognizing the possible threat and the impact of cyber attacks on Ethiopian economy, the government of Ethiopia engaged in several initiatives to secure safe cyber space. Some of these initiatives are:

- Formulated legal framework to secure cyberspace: Telecom fraud offence proclamation No. 761/2012.
- Develop and implement Cyber security affiliated national information and communication technology policy and strategy.
- Develop and implement national spatial information and technology policy.
- Established Information Network Security Agency with council of Ministers Regulation No. 1340/2006 and
- Prepare and enforce Critical Mass Cyber Security Requirement Standard /CMCSRS/ version 1.0.

The Ethiopian government issued a legal framework for telecom related offence in 2012. The telecom fraud offence proclamation No.761/2012 stated three main reasons for this legislation. These three premises for this legislation are:

- the increase and wide spread telecom related offences in the country and the potential of telecom industry for the implementation of peace , democratization and development program of the country ,
- recognizing the serious impact of telecom fraud to the national security beyond economic losses,
- and to adequately address the gap of the previous legislation in relation to telecom offence.

The first and main initiative of Ethiopian government in Cyber security is Telecom fraud offence proclamation No. 761/2012. Telecom fraud offence proclamation No. 761/2012 contains three parts. The first part of the proclamation contains two articles which mainly covers the title of the proclamation and definition of related words or phrases. The second part of the proclamation deals with telecom fraud offences. This part has 10 main articles and sub articles. These articles covers offence related to telecom equipments, services, interceptions and access, illegal use, fraud related to service charge and call-back. Based on the offence, the legislation recommends a prison term ranges from 1 to 15 years and a fine. The last part of this proclamation, Miscellaneous provisions contains 7 articles and sub articles. These articles deal with establishment of technical task force, covert search and admissibility of evidence.

The second initiative of the Ethiopian government is the establishment of Information Network Security Agency /INSA/.The Ethiopian government established INSA in 2006 with council of ministers Regulation no 130/2006. According to this proclamation of article 5, INSA is established with the basic objective of ensuring the country's use of information and information communication network technologies and telecommunications in the implementation of its peace, democratization and development program executed without risk to the national security.

The agency has vast powers and duties as stated in its establishment proclamation of article 6. It is responsible for advising the government on information communication network security and

monitoring the implementation of approved policies and legislation. It is also responsible for creating national research and development capability in information communication network technology and information warfare.

There are also other initiatives taken by Ethiopian government to secure safe cyberspace. These are Cyber security affiliated national information and communication technology policy and strategy, national spatial information and technology policy and the preparation and implantation of Critical Mass Cyber Security Requirement Standard /CMCSRS/ Version 1.0. The next portion discusses Critical Mass Cyber Security Requirement Standard /CMCSRS/ Version 1.0.

2.5.1 Critical Mass Cyber Security Requirement Standard /CMCSRS/ Version 1.0

INSA released Critical Mass Cyber Security Requirement Standard Version 1.0 in 2016. CMCSRS version 1.0 stated that governmental and nongovernmental organizations in Ethiopia are highly relying on information and communication technology, and information is becoming invaluable economic, political and social asset of the nation and a resource to transform the economy (p.7). This requirement standard acknowledges the security threats associated with information technology. The standard clearly stated this as, the reliance on information systems in increasing the vulnerability of the organization to cyber attacks are becoming highly complicated, dynamic and destructive (CMCSRS version 1.0, 2016, p.7). It further stated that it is essential to ensure the security of organizational information systems in order to protect organizations from attacks and minimize the impact of attack on the country. Due to this reason , CMCSRS version 1.0 is issued by INSA pursuant to article 13 of INSA re-establishment proclamation execution council of Ministers Regulation No. 320/2014 (CMCSRS version 1.0,2016,p.7).

The main objective of this standard is to ensure the critical information and information systems of the country in order to protect our national interest .This CMCSRS version 1.0 is prepared for all government institutions, and critical infrastructures like EEP, EEU and Ethio Telecom. This standard contains activities and processes in four categories namely:

- An absolute Requirement : means requirement is mandatory,

- An absolute Prohibition,
- Highly Recommended.
- And not recommended (CMCSRS version 1.0, 2016, p.14).

In this standard, a cyber security management model has been developed to express the concept of the critical mass cyber security requirement standard. This model contains three dimensions:

1. Perspective Dimension (D1): this dimension contains capability building, process, stake holders and mission perspective of cyber security.
2. Level Dimension (D2): this dimension contains strategic, tactical and operational levels of cyber security.
3. Analysis Dimension (D3): this dimension is applied to analyze cyber security at strategic, tactical and operational levels of capability building, processes and stake holders and mission. The strategic level can be analyzed using SGOC (Strength, Gap, Opportunity and Challenge) with PESTLE (Political, Economic, Social, Technological, Legal and Environmental) in it. The tactical level can be analyzed using BMIS (Governance, Process, people, technology and the six dynamic interconnections). The operational level can be analyzed using operation related clauses of ISO 27001(operation, support and other relevant clauses)(CMCSRS version 1.0, 2016, p.18-19). Figure 2.2 shows cyber security strategic Management model of the standard.

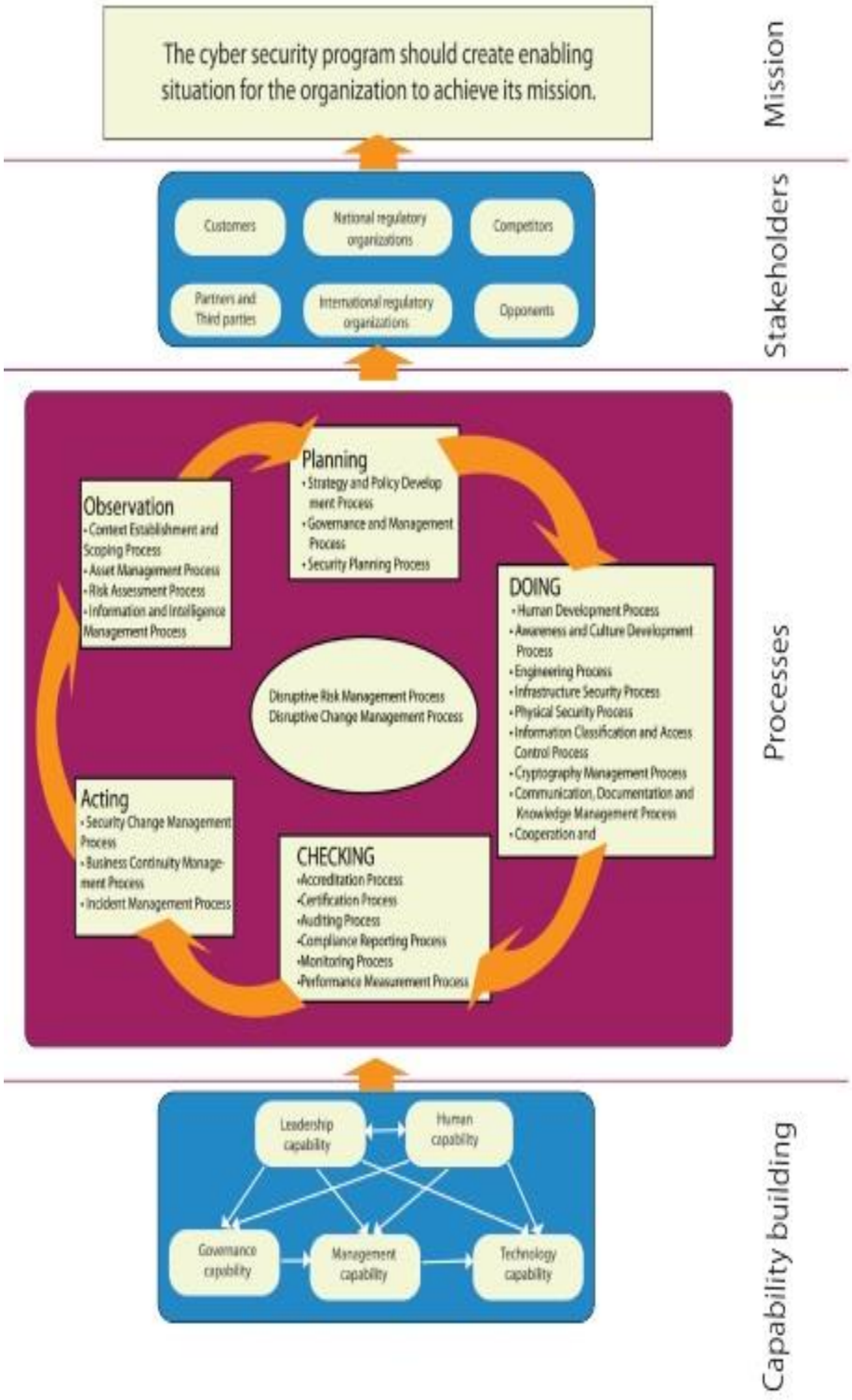


Figure 2.2 cyber security strategic Management model (INSA's CMCSRS version 1.0, 2016, p.19)

According to CMCSRS of 2016 the core principles of the security strategic model are:

- Risk based: organization should implement cyber security solutions/controls/ based on risk assessment,
- Embedded security: organization should embed cyber security in their organizational structures and processes,
- Cost effective ,
- Focus on human, process and structure, and
- Balanced and aligned with national cyber security and directives (CMCSRS, 2016, p.21-25).

In addition the standard stated that it should be used as a tipping point. The CMCSRS stated this concept as organization should identify 80-20 in each area and focus on the 20% based on 80 -20 rule (Pareto Principle) (CMCSRS, 2016, p.21-25). This provides an area to maneuver cyber security framework based on organization specific events and risk.

The strategy and methodology of the standard stands on the following pillars:

- OPDCA with RACI in it: observe, plan, do, check and act/OPDCA/ cycle will be used in cyber security capability building and processes, and Responsible, Accountable, [To be] consulted and [To be] informed /RACI/ bodies will be identified at each stage.
- Top down leadership
- Centralized and distributed responsibility, and
- Strong and strict regulation and institutionalism mechanism (CMCSRS, 2016, p.23-24).

The standard further identified four focus areas: Capability building, Processes, Stake holders and mission. The objective of capability building focus area is creating dynamic and continually learning cyber security tasks of the organization (CMCSRS, 2016, p.27). The following figures show capability building framework and architecture.

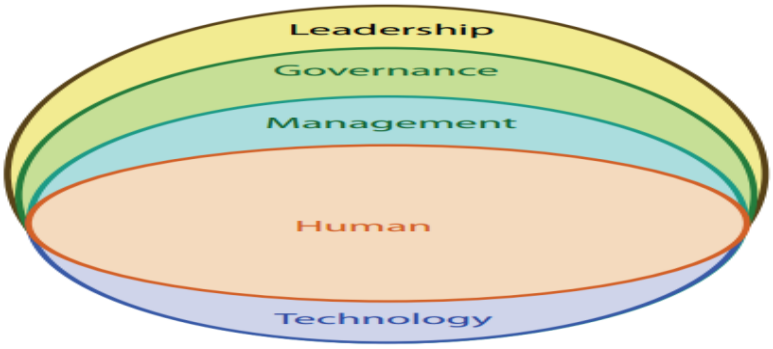


Figure 2.3 Capability Building Framework.

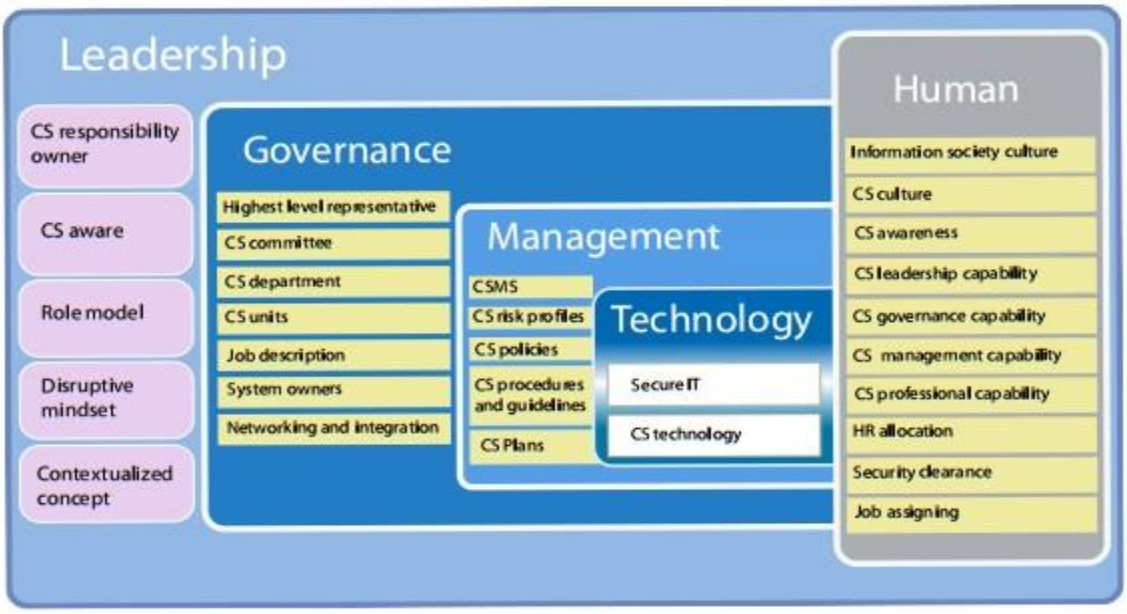


Figure 2.3 Capability Building Architecture.

The second focus area of the standard is the processes. The process framework consists of four categories: strategic management process, core processes, enabling process and disruptive processes(CMCSRS,2016.p45). Figure 2.4 shows the process framework.

Figure 2.4 shows CMCSRS the process framework.

According to the CMCSRS the process cycle contains five processes: observation, planning, doing, checking, and Acting /OPDCA/. Figure 2.5 shows the OPDCA process cycle (p.47).

Figure 2.5 shows CMCSRS the OPDCA process cycle

Third focus area of the standard is stake holders. The standard clearly stated that the organization should address stake holders' security requirement (of customers, partners and third parties, national regulatory organization, international regulatory organization, competitors' and opponents). The final focus area of the standard, Mission, stated that the cyber security program should create enabling situation for the organization to achieve its mission (CMCSRS, 2016, p.107).

Even if the foundation of safe cyberspace is being built, there is no sector specific cyber security framework. Due to this attempt is made to propose a tailored Cyber security framework based on NIST framework for improving critical infrastructure Cyber security draft 1.1 and INSA's Critical Mass Cyber Security Requirement Standard version 1.0. In the next section global Cyber security index 2017 and NIST framework for improving critical infrastructure Cyber security version 1.1 is briefly discussed.

2.6 Global Cyber Security Initiative

Global Cyber Security Index / GCI/ (2017) stated that the global community is increasingly embracing ICTs as key enabler for social and economic development. It further stated that governments across the world recognizes that digital transformation has the power to further the prosperity and well being of their citizens (p.iii). However these enablers came with the possible threat for social, economic, and political well being for every nation. Due to this GCI (2017) affirmed that governments recognize that cyber security must be an integral and indivisible part of technological progress (p.iii). There are several global Cyber security initiatives. Some of these are the Accenture security index, Cyber security poverty index, IBM X-force threat intelligence index 2017, index of Cyber security and Global Cyber security Index. This research is based on the International Telecommunication Union /ITU/ Global Cyber Security Index /GCI/ three pillars namely legal, Technical, and capability building. These pillars and their sub pillars of Global Cyber Security Agenda /GCA/ are used in this research to identify the practices and the challenges of cyber security at selected critical infrastructure in Ethiopia. Therefore the following section discusses these pillars of Global Cyber security Agenda/GCA/.

2.6.1 Global Cyber Security Index /GCI/ 2017

GCI is an initiative of International Telecommunication Union/ITU/.GCI of 2017 report stated that GCI was first launched in 2014 with the goal of helping to foster a global culture of cyber security and its integration at the core of ICTs. The second iteration of GCI at 2017 measures the commitment of ITU 193 member states towards cyber security in order to drive further efforts in the adoption and integration of cyber security on a global scale. GCI revolves around the ITU Global Cyber Security Agenda /GCA/ and its five pillars (legal, technical, organizational, capacity building, and cooperation).

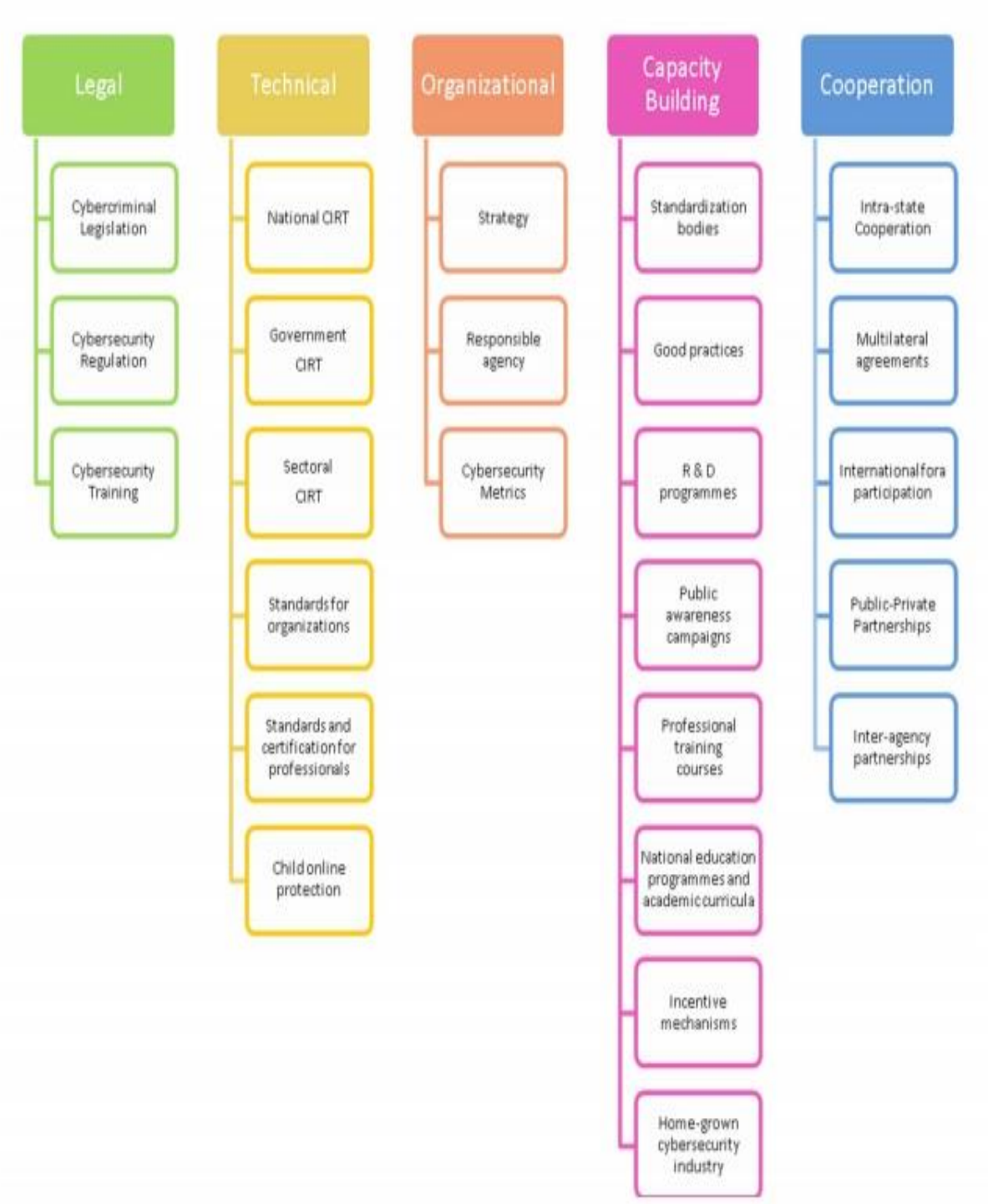


Figure 2.6 GCI pillars and Sub- pillars (Global Cyber Security Index, 2017, p.5)

In order to achieve the required level of granularity and ensure accuracy and quality of answers, GCI 2017 used an online questionnaire which contains 25 indicators and 157 binary questions on GCA pillars and sub pillars (Global Cyber Security Index, 2017, p.5).

2.6.2.1 The Legal Pillar

According to GCI 2017 the legal pillar used to measure the existence of legal institutions and frameworks dealing with cyber security and cyber crime. The legal pillar deals with cyber crime law, procedural law, and cyber legislation (p.5).

2.6.2.2 The Technical Pillar

GCI 2017 report used this pillar to measure the existence of technical institutions and frameworks dealing with Cyber security. The technical pillar deals with the existence of computer incident response team / CIRT/ at national, governmental and sectoral level. Moreover this pillar refers to the existence of standards for organizations and certification for professionals. Furthermore the technical pillar measures the existence of child on line protection (p.5).

2.6.2.3 The Organizational Pillar

This is used to measure the existence of policy coordination institutions and strategies for cyber security development at the national level. The organizational pillar contains three sub pillars namely strategy, responsible agency and cyber security metric (Global Cyber Security Index, 2017, p.5).

2.6.2.4 The Capacity Building Pillar

This pillar is used to measure the existence of research and development, education and training programs; certified professionals and public sector agencies fostering capacity building. The capacity building pillar contains eight sub pillars:- standardization body , good practices , R & D programs, public awareness campaigns , professional training courses national education and academic curricula , incentive mechanism and home grown cyber security industry (Global Cyber Security Index, 2017, p.5).

2.6.2.5 The Cooperation Pillar

The cooperation pillar measures the existence of partnerships, cooperative frameworks and information sharing networks. This pillar contains five sub pillars namely intra-state cooperation, multilateral agreement, international participation, public-private partnership and inter-agency partnership (Global Cyber Security Index, 2017, p.5).

2.7 NIST Framework

According to USA patriot act of 2001 critical infrastructures are institutions, systems or assets, whether physical or virtual that the incapacity or destruction would have a debilitating impact on security, health, safety or the combination of those matters. This holds true in Ethiopian context. Some of the critical infrastructures in Ethiopia are Ethiopian Electric Power, Ethiopian Electric Utility, and Ethio Telecom. The security breach of any type and magnitude on these critical infrastructures would have a devastating effect on the economy, social and political sphere.

This research reviewed three cyber security frameworks in order to select an existing framework to tailor a framework for critical infrastructures in Ethiopia. The first framework reviewed is a framework for aviations cyber security. This aviation cyber security framework which is formulated in 2017 stated that its objective as

- Establish common cyber standards for aviation systems,
- Ensure a cyber security culture ,
- Understand the threat,
- Understand the risk, and
- Communicate the threats and assure situational awareness.(The Worlds forum for aerospace Leadership 2017 The connectivity Challenge : Protecting Critical Assets in Networked World, A Framework for Aviation Cyber Security, p.6-7).

Even thought this framework provides remedy for aviation, it is more specific to that sector. Therefore is not suitable to tailor it for other sectors for technology and electric power and distribution.

The second cyber security framework reviewed for this research is a framework for cyber security information sharing and risk reduction. This framework is initiated by Microsoft Cooperation and developed by Cristin Goodwin and J. Paul Nicholas in 2015. This framework identified cyber security stakeholders or actors and their role and type of cyber security information. However this framework only deals with cyber security information sharing and risk reduction in information sharing. Therefore it is not suitable for over all processes at critical infrastructure in Ethiopia.

The third framework reviewed and selected to tailor a framework is NIST framework for improving critical infrastructure cyber security version 1.0. NIST framework (2017) stated that Cyber security threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's economy and public safety and health risks (p.5). In recognizing the need to protect critical infrastructures, National Institute Standards and Technology /NIST/ prepared and released a framework for improving critical infrastructure Cyber security draft version 1.1 on January 10, 2017. However, the framework for critical infrastructure is different among countries and institutions. NIST framework (2017) stated that the framework is not a one-size-fit all approach to managing Cyber security risks for critical infrastructure. It is also stated that organizations will continue to have unique risks-different threats; different vulnerabilities, different risk tolerance – and how they implement practices in the framework will vary (p.6). However the framework is aimed at reducing and better managing Cyber security risks. The framework focuses on using business drivers to guide Cyber security activities and considering Cyber security risks as part of the organizations risk management process.

The NIST framework consists of three parts:

- The framework core
- The framework profile
- And the implementation tiers (NIST framework for improving critical infrastructure Cyber security, 2017, p.5).

The first part of NIST framework, i.e the framework core is a set of Cyber security activities, outcomes and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational profiles. The core presents industry standards, guidelines and practices in a manner that allows for communication of Cyber security activities and outcomes across the organization from the executive level to the implementation /operation/ level (NIST framework for improving critical infrastructure Cyber security,2017,p.5).The framework core consists of five concurrent and continuous functions:

1. Identify: develop the organizational understanding to manage Cyber security risks to systems, assets, data and capabilities. The activities in the identify function are foundational for effective use of the framework.
2. Protect: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The protect function supports the ability to limit or contain the impact of a potential Cyber security event.
3. Detect: develop and implement the appropriate activities to identify the occurrence of a cyber security event. The detect function enables timely discovery of Cyber security event.
4. Respond: develop and implement the appropriate activities to take action regarding a detected Cyber security event. The respond function supports the ability to contain the impact of a potential Cyber security event.
5. Recover: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a Cyber security event (NIST framework for improving critical infrastructure Cyber security, 2017, p. 5-9).

The second part of the NIST framework is framework implementation tiers. This part provide context on how an organization views Cyber security and the processes in place to manage that risk. The last and the third part of NIST framework is framework profile. Framework profile represents the outcomes based on business needs that an organization has selected from the framework categories and subcategories (NIST framework for improving critical infrastructure Cyber security, 2017, p.9).

2.8 Related Works

There are several empirical researches in areas of cyber security. In this portion two cyber security related researches are discussed. The first empirical research selected for discussion is conducted by Halefom Hailu in May 2015 with the title of "The state of Cyber Crime Governance in Ethiopia". In this article attempts were made to explore the efforts and initiatives made by the government in fighting cyber crime from three cyber space governance perspectives: cyber security – related policies and strategies, legislative frameworks, and institutional arrangements. Based on the empirical data collected and close examination of the

legislations and policies , the study recommended on what plans and measures the government can implement in pursuit of safer and secure Ethiopia (The state of cyber crime governance in Ethiopia,2015,p.1). Hailu (2015) built a conceptual framework for the article by citing the related works of several scholars.

Anja Mihr (2013) stated that nowadays cyber space has become so omnipresent that some have begun to employ the language of nation hood to describe it. If cyber space were a country, it would be the largest and most populated country in the world (As cited by Hailu, 2015, p.2). In further strengthen this concept the increase of network connection at a global level UNODC in its study entitled "Comprehensive study on cyber crime "of February 2013 stated that it is estimated that, by the year 2017, mobile broad band subscriptions will approach seventy percent of the world's total population and, by the year 2020, the number of networked devices will outnumber people by six to one, transforming current conceptions of the internet (As cited by Hailu, 2015, p.2). Therefore the effect of technology is increasing time to time. Hailu (2015) stated this as technology is, however neutral, and can empower those who build and those who destroy alike. He further explain this as with every new invention technology will always have its optimists who only see its potential to do good and its critics who only see its potential to do evil (p.2). He further stress that almost all traditional crimes can also be perpetrated from the online environment. Millions of people are victims of cyber crime every day and suffer trillions of dollars in loss worldwide. Hailu(2015) further raised that as never before, and at insignificant cost, ordinary citizens can cause calamitous harm to individuals, companies, and governments from places unknown. The threat of cyber crime has reached the level of national security concern (p.2). At the end of 2013, TREND micro incorporated published a report entitled "Africa: A new safe Harbor for cyber criminals?" gave three reasons for identifying Africa as a potential cyber crime safe heaven:

1. The availability of faster and more affordable internet access,
2. The expanding internet user base, and,
3. The lack of cyber crime laws (As cited by Hailu, 2015, p.6).

Jerome(2012) stated the situations in Africa related to cyber crime Africa as a continent is therefore vulnerable to a range of online criminal activities and becoming a major source of

cyber crime in the global information society (As cited by Hailu, 2015,p.2).Hailu (2015) stated that Ethiopia is no exception. On one hand, the country is experiencing a massive increase in internet access, and its internet user base is expanding. On the other hand, cyber security governance is at its embryonic stage, and much needs to be done. He further stated better and faster ICT services, however, open opportunities for cyber crime. The pervasiveness of mobile phones throughout the country, the introduction of new services such as mobile money, and financial services such as ATMs will also provide new opportunities for cyber criminals (p.7).

In this research, the researcher used a survey research method specifically questionnaire to collect data from different organizations. Hailu (2015) stated that the purpose of the questionnaire was to investigate the realities of cyber crime at organizational level and examine how the institutions are vulnerable to the threat of cyber crime (p.7). Even if the researcher do not specifically state what sampling technique he used, he stated that data were collected from forty institutions familiar with the uses of ICT with a response rate of 87.5%. The respondents were from private and government institutions including seventeen banks, twelve ICT institutions, and six other institutions such as federal governmental agencies, media, and transport (p.7).

After analyzing the data, Hailu (2015) found that all respondents experienced a number of cyber crime incidents. Computer viruses, warms, malware and other malicious attacks (57.1%), website defacement (40%), illegal access (17.1%) and spam (14.7%) were most frequently perpetrated cyber crimes against the institutions (p.8). The respondents also indicated a range of infrequently occurring cyber crime such as causing damage to computer data (62.9%), denial of service (DoS)(45.7%), and system interference (45.7%).

He concluded that overall, the survey results demonstrate that cyber crime is legitimate problem in Ethiopia (p.8). This article also shows that the 77% studied organizations do not have organizational structure dealing with cyber security. Only 8.6% of the institutions (three banks) have specialized teams responsible for cyber security incidents. He concluded that these results demonstrate that cyber security governance is neglected by the majority of the institutions involved in the survey (p.8). Moreover Hailu (2015) in his survey identified that while more than

half of the institutions said that they do not report at all, 25.7% said they report only major cyber attacks, most of them related to banking fraud. The survey provides some reasons for this reluctance, including the general belief that law enforcement is not capable of dealing with cyber crime (37.1%) and fear of adversary publicity (25.7%). There are even organizations (11.4%) who believe that the solutions for cyber security incidents are technical and hence out of law enforcement jurisdiction (p.9).

In addition to the survey, this article described the state of cyber crime governance in Ethiopia from aspect of policy measures. The three main policy measures described in this article are the national ICT policy and strategy of 2009, the growth and transformation plan (GTP 2010/11-2014/15) and institutional regulatory mechanism. Hailu (2015) stated that in 2009, the Ethiopian government adopted a general ICT policy and strategy with cyber security implications (p.10). The development of ICT and telecommunication infrastructure is one of the strategic pillars of GTP. In aspect of institutional regulatory mechanisms, the Ethiopian government established INSA in 2006 by Council of Ministers Regulation No. 130/2006. Hailu (2015) further stressed that INSA is the sole cyber security organ in Ethiopia (p.12).The article further discusses the existing legal framework starting from the FDRE criminal code 2004.

The second empirical research selected for this research is conducted by MIT Technology review custom in partnership with Hewlett Packard Enterprise security services and fire eye in 2016 with the title of "Cyber security challenges, risks, trends, and impacts". In this survey two hundred and twenty-five business and IT executives, directors, managers and other leaders participated in online survey, which was conducted by MIT technology review in partnership with Hewlett Packard Enterprise (HPE) security services and Fire Eye (MIT technology Review, 2016, p.1).

The survey indicated the top three information–security challenges: lack of in-house expertise (40%), inadequate enabling technologies (34%) and insufficient funding (27%). Mobile computing, employee mobile-device or application (BYOD/BYOA), attacks via e-mail and web are the fastest growing threat to information security. 34% of the respondents indicate that there are more attacks than two years ago. This indicates that the security threats are increasing

through time. Based on the Lickert scale, the respondents indicated that the organizations are somewhat prepared (Lickert scale of 3) concerning breach preparedness. The survey shows that it is only 40% of the organization that have information risk management strategies. Concerning the impact of the breach, the respondents indicated that lost time and productivity, remediation time and cost of purchased technologies are the main effect.

In this research, several key themes have emerged from analysis of the survey results. These are:

- Few survey participants are fully confident about their ability to respond to security threat.
- Many struggle to hire and retain highly qualified security specialists. Luck of in-house experts ranks as the single greatest information- security challenge, cited more than one-third of the participants.
- Most lack information risk management strategies. Although many expect to develop them, roughly 25% either have no plans to do so or simply don't know whether their organizations have or eventually will have such strategies.
- Most see multiple security threats on the rise. Areas of greatest concern include threats related to mobile computing, e-mail, or web based attacks, and the vulnerabilities created by the bring-your own- device(BYOD) and bring-Your-Own App(BYOA) work place trend.(The MIT technology Review,2016,p.2-15)

The above two survey researches indicated that cyber security should be given due consideration by organizations and nations at large. The increase of cyber attacks on organizations is highly threatening the existence of the entities. Therefore organizations should be prepared and respond to any cyber attacks in a timely and appropriate manner. Due to this, this thesis attempts to identify the challenges and practices of cyber security at the critical infrastructures in Ethiopia. Moreover, in this thesis attempts are made to propose a tailored cyber security framework based on NIST cyber security frame work version 1.1 and INSA's Critical Mass Cyber Security Requirement Standard Version 1.0. Some of the pervious researchers done in cyber security are presented in the following table.

No	Author and Date of Publication	Title	Objectives	Findings
1	Tine Hojsgaard Munk (2015). A Thesis Submitted to the university of Manchester for Doctor of Philosophy in the faculty of Humanities.	Cyber-security in the European Region: Anticipatory Governance and Practices.	The aim of this research is to offer a greater insight in to the different forms of cyber security governance.	The author analyze anticipatory governance and practices in European region, which are determined by the geographical position and cooperative regionalism considered for their involvement in three European Security institutions- North Atlantic Treaty Organization, The council of Europe, and The European Union.
2	E Krizinger and SH Von Solms(2012). A research article published at Journal of Information Assurance & Cybersecurity.	A Framework for Cyber security in Africa.	The objective of this paper is to propose cyber security framework to assist Africa in increasing its cyber crime rate especially among home users with no or limited cyber safety knowledge.	The authors identified four major safety concerns in Africa discussed in recent literature. Based on these four major cyber safety concerns, the authors proposed a framework for cyber security in Africa.
3	Aychiluhim Desta and Tibebe Besha (2014). A resecrh article published at HiLCoE Journal of Computer Science and Technology, Vol. 2, No. 2	Internet Banking Security Framework: The case of Ethiopian Banking Industry.	To recommend holistic Multi-layered security that stretches towards client's side security and national financial and security.	The internet banking security framework and its major five security models have been developed and evaluated through expert evaluation method.

4	Yeboah-Boateng, Ezer Osei(2013). Thesis Submitted to Aalborg Univesitet Denmark for Doctor of Philosophy.	Cyber security Challenges with SMEs in Developing economies: issues of Confidentiality, Integrity, and Availability(CIA)	To mitigate the impact of cyber security compromises of Confidentiality, Integrity and Availability against their assets in developing economies.	Build a cyber security vulnerability assessment (CSVA) model and enlisting taxonomies of vulnerabilities and threats.
5	Halefom Hailu(2015). An Empirical Research Article.	The State of Cyber Crime Governance in Ethiopia	Attempt to explore the efforts and initiatives being made by the government in fighting cyber crime from three cyber space governance perspectives: cyber security-related policies and strategies, legislative frameworks, and institutional arrangements.	Provided recommendations on what plans and measures the government can implement in pursuit of a safer and secure Ethiopia.

Table 2.1 Related Works

2.9 Chapter Summary

Cyber security is a broader concept than information security and computer security. Several threat actors are involved in Cyber security breaches. Some of these Cyber security breach actors are hackers, hactivisim, criminal groups, state and state affiliated proxies, well meaning and malicious inside users.

There are different types of hackers based on their intention. These are black hat hackers, white hat hackers and gray hat hackers. Black hat hackers breach security with the intention of acquiring financial benefit or self gratification. However the white hat hackers, sometimes refer

as ethical hackers, their intention is the opposites of black hat hackers. These categories of hackers are paid IT professionals which test and inform organizations about their security weakness by hacking in to cooperate network. The gray hat hacker intension lies in between the black hat hackers and the white hat hackers. The second category of Cyber security threat actors are hacktivism. The term hacktivism is the combination of the term “Hack” and “activisim”. Hacktivism falls in to the grey area between politics and crime. The last two Cyber security threat actors are well meaning insiders and malicious insiders. These threat actors used different methods to breach security. Some of these methods are social engineering, denial of service, distributed denial of service, web site defacement, malware, viruses, and spyware. These threat actors attack companies in developed and developing countries.

Ethiopia as a developing nation should be in a position to avert these threats and attacks mainly on critical infrastructures. Ethiopian government took several steps to ensure safe cyberspace. Some of these initiatives are Telecom fraud offence proclamation No. 761/2012, Cyber security affiliated national information and communication technology policy and strategy, national spatial information and technology policy, established Information Network Security Agency with council of Ministers Regulation No. 1340/2006 and Critical Mass Cyber Security Requirement Standard /CMCRS/ version 1.0.

Similarly there are several global Cyber security initiatives. One of this Cyber security initiative is Global Cyber Security Index which prepared index on counties commitment on Cyber security. The second initiative is the initiative of NIST. NIST prepared and released NIST framework for improving critical infrastructure Cyber security draft version 1.1. This research investigates the practices and challenges of Cyber security based on global Cyber security’s five pillars and NIST framework’s five framework core functions. Moreover this research proposes a tailored Cyber security framework based on NIST framework critical infrastructures Cyber security draft version 1.1.

CHAPTER THREE

Research Methodology

3.1 Overview

This research targets to identify and examine practices and challenges of Cyber security at three selected critical infrastructures in Ethiopia. The research also proposes a tailored Cyber security framework based on the NIST /National Institute Standards and Technology / framework for improving critical infrastructures for Cyber security version 1.1 and INSA's Critical Mass Cyber Security Requirement Standard Version 1.0.

A sound research depends on the methodology it follows to answer the research questions. Research methodology is defined by Leedy & Ormod (2001) as general approach the research takes in carrying out the research project (As cited by Williams, 2007, p.1). In order to address the research questions, this research uses quantitative, qualitative approaches and design science guidelines to tailor cyber security framework.

Gable, Guy G (1994) stated the value of combining quantitative and qualitative research methods in IS research (p.1). Moreover this research uses Hevner et al. seven guide lines of design science in order to tailor cyber security framework. Hevner et al. (2004) prepared seven guidelines in the building and application of an artifact (p.82). Accordingly in this research, the seven guide lines are considered and followed in tailoring the cyber security framework for critical infrastructures.

In the next sections the general approach of the research, the research pillars and sub pillars, the three selected critical infrastructures and the study population, data collection methods, analysis and procedures, pilot testing on data collection instruments, and validity and reliability of the research is presented.

3.2 General Approach

Williams (2007) stated that research originates with at least on one question about phenomenon of interest (p.1). This research targets to answer three questions as stated in chapter one sub

portion 1.3. Williams (2007) further stated that research questions, help researchers to focus thoughts, manage effort and choose the appropriate approach or perspective from which to make sense of each phenomenon of interest (p1).

This research uses quantitative, qualitative research approach and design science guide lines to tailor the cyber security framework. The research uses quantitative research approach in order to identify the challenges of Cyber security at the selected three critical infrastructures. This approach enables to identify the existing challenges from the population by using questionnaire as an instrument. Williams (2007) affirmed that researchers typically select the quantitative approach to respond to research questions requiring numerical data (p.1). Accordingly this research targets to identify the numerical impact of Cyber security challenge from the population of study at each critical infrastructure.

Rahi S. (2017) stated that qualitative approach is used to collect the in-depth details on a particular topic (p.2).Williams (2007) stated that one identifier of a qualitative research is the social phenomenon being investigated from the participant's view point. He further stated that what constitutes qualitative research involves purposeful use for describing, explaining and interpreting collected data (p.3). This research uses qualitative research approach using interview data collection instrument in order to clearly identify the practices of Cyber security and to propose and evaluate tailored Cyber security framework for selected critical infrastructures.

Therefore this research uses both quantitative and qualitative research approaches. Due to this, the research simply uses a mixed research approach. Williams (2007) stated that with mixed methods approach to research, researchers incorporate methods of collecting or analyzing data from the quantitative and qualitative research approach in a single research study. He further stated that goal for a researcher using the mixed methods approaches to research is to draw the strengths and minimize the weaknesses of the quantitative and qualitative approaches (p.7). Both research methods are not only compatible but also complementary.

This research also uses the design science seven guidelines in order to tailor the cyber security framework for the selected critical infrastructures. Because designing an IT artifact like a model

or framework is not a random process. Hevner et al.(2004) proposes seven guidelines in building and application of an artifact(p.82). These guidelines are Design as an artifact, problem relevance, design evaluation, research contributions, research rigor, design as a search process and communication of research. Accordingly this research follows these seven guidelines in tailoring the cyber security framework for the selected critical infrastructures.

Based on the experience of US home land security and the US patriot act definition of critical infrastructure, this research identified the following critical infrastructures in Ethiopian context. These are Ethiopian Telecom, Ethiopian Electric Power and Ethiopian Electric utility. These critical infrastructures are the case study for this research. The case study enables researchers to have in depth understanding of Cyber security in Ethiopian context.

Benbasat et al (1987) identify three strengths of case study research in information systems:

(1) The researcher can study information systems in a natural setting, learn about the state of the art, and generate theories from practice;

(2) The method allows the researcher to understand the nature and complexity of the process taking place; and

(3) Valuable insights can be gained into new topics emerging in the rapidly changing information systems field (As cited by Gable, Guy G, 1994, p.3).

The following Flowchart shows the simplified research process.

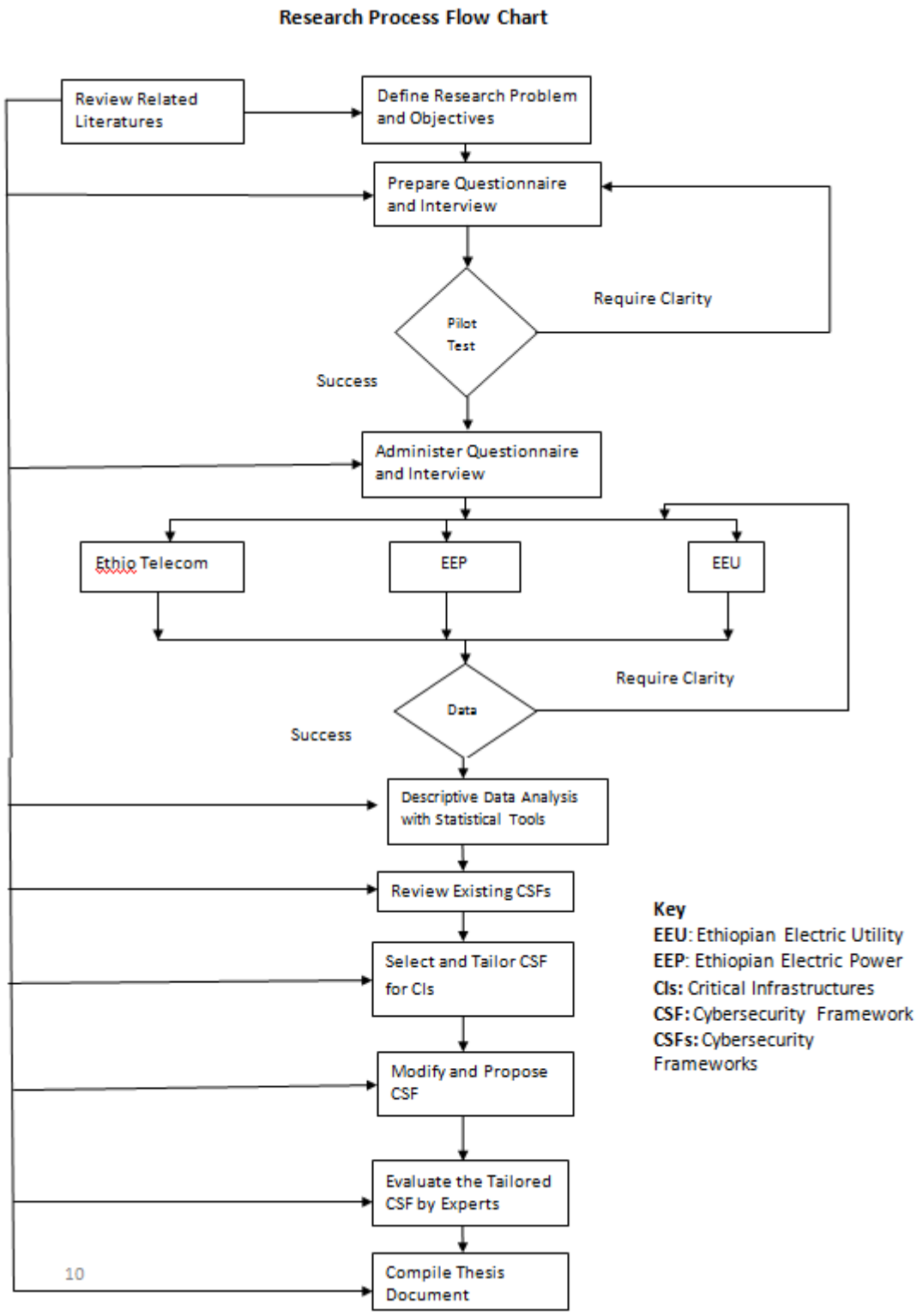


Figure 3.1 Simplified Research Process

3.3 Research Pillars and Sub Pillars

There are several global Cyber security initiatives. As it is discussed in chapter one, one of these initiatives is the Global Cyber Security Index/GCI/. GCI was first launched in 2014 with the goal of fostering a global culture of Cyber security and its integration at the core of ICTs.GCI measures the commitment of International Telecommunication Union's /ITU/ 193 member states commitment towards Cyber security in order to derive further efforts in the adoption and integration of Cyber security on a global scale.

The GCI revolves around the ITU's Global Cyber security Agenda /GCA/ and its five pillars (Global Cyber security Index 2017, p.iii). These pillars are legal, technical, organizational, capacity building and cooperation. These pillars are used to measure ITU's member states commitment towards Cyber security using 157 binary questions and 25 indicators. GCI identifies the existence and lack of pillars and sub pillars by using questionnaire and open source research.

This research adapts three of these pillars (Legal, Technical and capability Building) and modified the sub pillars based on National Institute of Standards and Technology /NIST/ Framework for improving critical infrastructure Cyber security version 1.1. Because the existence or lack of a certain pillar or sub pillar in relation to Cyber security cannot clearly show the practices and challenges of Cyber security at the three critical infrastructures in Ethiopia as it was the case for GCI of 2017.

NIST framework draft version 1.1 (2017) is a framework for improving critical infrastructure Cyber security. The NIST framework for critical infrastructure consists of three parts: the framework core, the framework profile and the implementation tiers. The framework core is a set of Cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing organizational profile (framework for improving critical infrastructure Cyber security version 1.1, 2017). The framework core consists of five concurrent and continuous functions: Identify, protect, detect, respond and recover. This research uses the framework core of NIST as a sub pillar for technical

pillar. The following diagrams show this research's pillars and sub pillars based on GCA's three pillars and NIST framework for improving critical infrastructure Cyber security version 1.1.

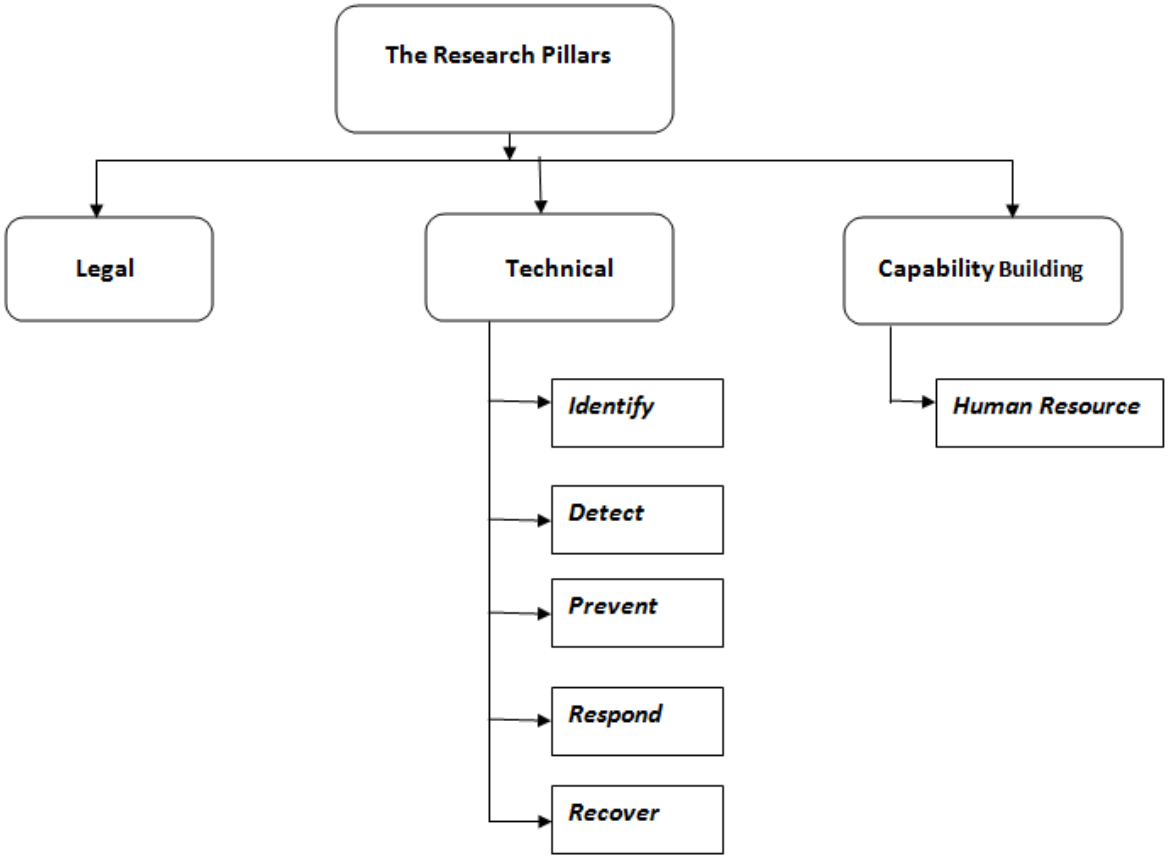


Figure 3.2 Three Pillars and sub Pillars used in this research

The three pillars of this research are briefly explained below:

1. Legal: investigates and examine cyber crime legislations, policies, institution and standards.
2. Technical: This pillar examines the practices and the challenges of cyber security based on NIST framework core i.e. Identify, protect, detect, respond and recover.
3. Capacity Building: studies institutions capability to recruit, develop, and retain security expertise and leader ship.

3.4 Study Population

This research studies Cyber security practices and challenges at three critical infrastructures in Ethiopia namely Ethiopian Electric Power /EEP/, Ethiopian Electric Utility /EEU/, and Ethio Telecom. The study considers the whole staff of Cyber security Units or IT Security and Compliance Units of each organization as study subjects. Therefore the population of the study is all Cyber Security or IT security technical and managerial staffs of each selected critical infrastructure. This is because total study subjects from the three organizations are 75; it's manageable and yields more accurate and consistent information on the practices and challenges of Cyber security.

3.5 Data Collection Techniques and Procedures

This research uses Semi-Structured Interviews and questionnaire for data collection. The semi-structured interview and questionnaire for this study is based on Global Cyber Security Index /GCI/ questionnaire guide of International Telecommunication Union/ITU/ and MIT Technology Review Customs. ITU used interview and questionnaire for preparing Global Cyber security Index 2017 /GCI/ based on the Five pillars of Global Cyber security Agenda /GCA/ from its Member States. These instruments are adapted and modified. Furthermore in order to study and examine the national effort in Cyber security, interview is conducted on Cyber security staff of Information Network security Agency / INSA /. Additionally the content of framework evaluation questionnaire is derived from the evaluation criteria recommended by Hevener (2004) which consists of fit to the organization, comprehensiveness, reliability, clarity, correctness, and usability quality attributes.

This Research reviewed NIST / National Institute of Standards and Technology/ framework for improving critical infrastructures Cyber security version 1.1, INSA's Critical Mass Cyber Security Requirement Standard Version 1.0 and tailored Cyber security framework for the three selected critical infrastructures for current and future challenges.

3.5.1 Ethiopian Electric Power and Utility

The former Ethiopian Electric cooperation is separated in to two independent entities namely the Ethiopian Electric Power and The Ethiopian Electric utility. Staff members in IT Security and

Compliance unit of the ICT department are considered as a population for this study. The following table shows the number of study subjects and the method of data collection used.

Job Category	**Level**	**Specific Title**	**Research Method To be used**
Management	Top level Manager	ICT Department Head	3 Semi-Structured Interviews
	Middle Level Managers	IT Operation and Support Unit Head	
		IT Security and Compliance Unit Head	
		IT Application Unit Head	
		IT Infrastructure /Hardware & Software / Unit Head	
IT / IT Security Professionals	IT Professionals from IT Security and Compliance Unit		25 Questionnaires

Table 3.1 Ethiopian Electric Power and Utility Study Population

3.5.2 Ethio Telecom

The Ethio Telecom information system division / ISD / has six departments. These are:

- IT service strategy & program management department
- IT service design department
- IT service transition department
- IT service operation department
- Office automation department and
- IT and Network security department

This research uses study subjects from IT and network security department. There are 50 IT professionals within IT and Network security Unit. The whole population is considered for this study. The details for data collection for interview and questionnaire are shown in the table below.

Job Category	**Level**	**Specific Title**	**Research Method To be used**
Management	Executives	ISD CIO	3 Semi-Structured Interviews
	Top level Manager	IT and Network Security Department Head	
	Middle Level Managers	IT Security Unit Head	
		Network Security Unit Head	
		Network Operation Center Unit Head	
		IT Fraud Operation Unit head	
IT / IT Security	IT Professionals		50 Questionnaires

Table 3.2 Ethio Telecom Study Population

Therefore for this research IT / computer security divisions of the three organizations are used for data collection. The total of 75 questionnaires and 6 interviews are used to gather data based on researcher's three pillars and sub pillars.

3.6 Data Analysis and Evaluation Technique

This research uses two categories of data analysis techniques; namely quantitative data analysis and qualitative data analysis techniques. Quantitative data analysis techniques are mainly applied to quantify items from questionnaire data collection instrument. This is because quantitative research creates meaning through objectivity uncovered in the collected data (Williams, 2007, p.2).Creswell(2003) stated that quantitative research involves the collection of data so that information can be quantified and subjected to statistical treatment in order to support or refute "alternative knowledge claims" (As cited by Williams,2007, p.14). Willams (2007) further stated that the findings from quantitative research can be predictive, explanatory and confirming (p.2). This research uses explanatory statistical techniques specifically percentages to analyze data collected using questionnaires.

There are numerous approaches for analyzing qualitative data (Elo S. &Kyngash , 2008). This research uses content analysis for qualitative data acquired from interview and document review. Cole (1998) stated that content analysis is a method of analyzing written, verbal or visual communication messages (As cite Elo S. &Kyngash , 2008, p1). This data analysis method is appropriate to analysis the content of the interview and the documents related to Cyber security. Elo S. & Kyngash(2008) stated this content analysis is also known as a method of analyzing documents (p.2). Content analysis can be used to develop an understanding of the meaning of communication (Cavanagh 1997) and to identify critical processes (Lederman 1991) (As cite Elo S. &Kyngash , 2008, p3).

Elo S. &Kyngash(2008) stated that content analysis may be used in an inductive and deductive way (p. 2). Burns & Grove (2005) stated that a deductive approach is based on an early theory or model and therefore it moves from the general to specific (As cite Elo S. & Kyngash , 2008, p3). This research uses deductive content analysis method for analyzing interview data, documents and to develop and evaluate tailored Cyber security framework based on NIST framework for improving critical infrastructure Cyber security version 1.1 and INSA's Critical Mass Cyber Security Requirement Standard Version 1.0.

Satu Elo & Helvi Kynga¨s (2007) stated that both inductive and deductive analysis processes are represented as three main phases: preparation, organizing and reporting (p.109). The same authors stated that deductive content analysis involves developing analysis matrix, data gathering by content, grouping, categorization, abstraction, and reporting the analyzed process (p.110). Accordingly this research identified four analysis matrix; cyber security challenges, cyber security practices, cyber security growth and cyber security framework. The results of the interview and document analysis further grouped in sub categories for the analysis.

Finally the tailored cyber security framework followed two processes build and evaluate. As it is discussed previously the seven guide lines of design science are used to tailor the cyber security framework. The tailored cyber security framework is evaluated using questionnaires, interview and expert evaluation. The tailored Cybersecurity framework is evaluated for its technical processes, suitability, comprehensiveness, clarity, correctness, completeness, and fitness to the

organization and its usefulness to combat cyber threats. Because Hevner(2004) stated that an IT artifact need rigorous evaluation with respect to functionality, completeness, reliability, usability, fit to the organization, and other relevant quality attributes prior to using it to the intended goal. According to Hevner (2004) an IT artifact can be evaluated by observational, analytical, experimental, testing, expert validation, and descriptive methods. Accordingly this research use descriptive evaluation using questionnaire and expert validation using interview is used to evaluate the tailored cyber security framework.

3.7 Reliability and Validity Testing

This research uses a pilot testing to examine the reliability and validity of questionnaire and interview by IT and network security professionals from the three selected critical infrastructures. Moreover the pilot testing on the reliability and validity of the questionnaire and the interview is conducted on staff of IT and network security professionals from Information Network Security Agency /INSA/ .

3.8 Chapter Summary

This research studies Cyber security practices and challenges at selected critical infrastructures in Ethiopia. These critical infrastructures are Ethiopian Electric Power, Ethiopian Electric Utility, and Ethiopian telecom. These infrastructures should be protected from cyber breach of any kind. The study examines Cyber security of these infrastructures from IT security professional from each institutions. In order to enhance the reliability and the validity of data collection the whole population of Cyber security units / IT security and compliance unit/ of each organization is included in the study. This research uses the five pillars of Global cyber security agenda and modifies the sub pillars based on NIST framework for improving critical infrastructures Cyber security version 1.1. The data is collected on these pillars and sub pillars.

The research uses both quantitative and qualitative research approaches. Explanatory data analysis method specifically percentages are used on quantitative data analysis from the questionnaire. Deductive content analysis method is used to analysis data mainly acquired from interview and questionnaires.

CHAPTER FIVE

Data Presentation, Analysis and Discussion

4.1 Overview

In this portion, the result of the survey is presented. This chapter is divided in to three sections. The first section contains three findings. These are demographic properties of the respondents, the challenges and growth trends in security threats. The second section presents the level of preparedness of cyber security threats and breaches at selected critical infrastructures. The final section contains revisit of research questions and cyber security practices: Legislations, Policies, Institution and Standard of cyber security in Ethiopia.

As it is discussed in chapter three, this is a case study of three critical infrastructures in Ethiopia. The three critical infrastructures are Ethiopian Electric Power/EEP/, Ethiopian Electric Utility/EEU/ and Ethio Telecom. Questionnaires and interviews are used to collect data from the selected critical infrastructures about cyber security practices and challenges. For the purpose of confidentiality, the critical infrastructures are given a code name. The following table shows the number of questionnaires distributed and the response rate.

Critical Infrastructures	No. of Questionnaires Distributed	No. of Questionnaires Returned	Percentage of Response Rate
CI #1	10	10	100
CI #2	15	13	86.7
CI #3	50	40	80
Total Response Rate in %	75	63	84

Table 4.1 Response Rate table

The overall response rate from the selected critical infrastructure surveyed is 84%. The reliability of the questionnaire is 0.892 Cronbach's Alpha which is considerably high. Table 4.2 shows reliability statistics on all 49 items.

Cronbach's Alpha	N of Items
.892	49

Table 4.2 Reliability Statistics of the Questionnaire

Moreover the interviews are conducted with six IT and Network security officers in order to validate the data and to identify the practices of Cybersecurity. Based on the findings, attempts are made to propose a tailored cyber security framework based on NIST framework to improve Cyber Security for Critical Infrastructures Version 1.1 and INSA's Critical Mass Cyber Security Requirement Standard Version 1.0.

4.2 Demographic Properties of Respondents

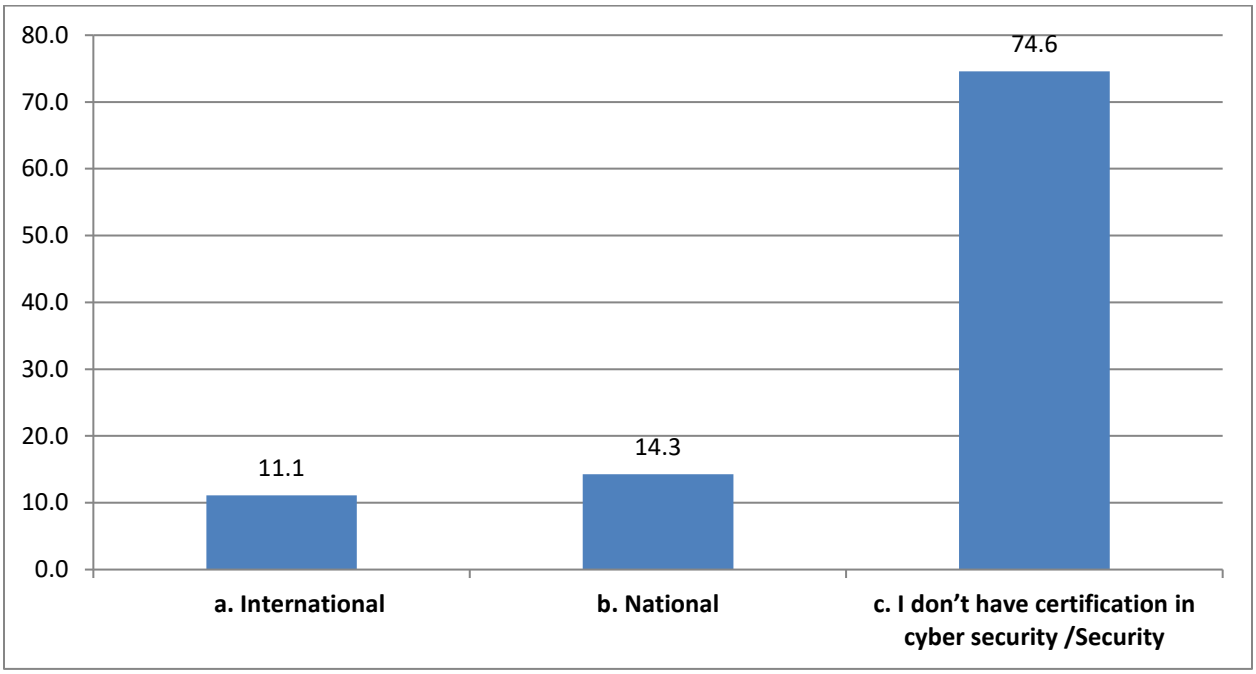
The questionnaire contains three demographic items specifically educational status (BSC, MSC, PHD or TVET level I-V), security certification (national, international or none) and year of experience.

Educational Status	Number of Employees	Percentage
PHD	0	0
MSC	13	20.6
BSC	49	77.8
TVET Level I-V	1	1.6
Total	63	100

Table 4.3 Educational Status Table

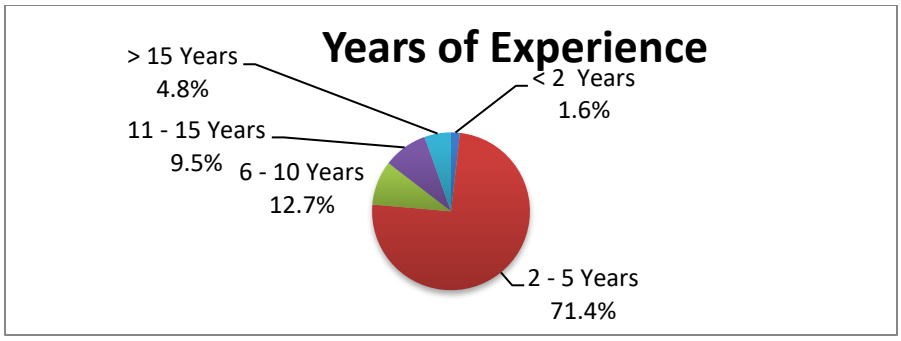
From the total respondents of security professionals at the selected critical infrastructures, 77.8 % and 20.6 % are BSC and MSc graduates respectively. These rates contribute significant share to the validity of the response and the level of security enforced. However it is not only the educational status but also the security certification and the number of years of experience within the organization contributes to cyber security at the critical infrastructures. Graph 4.1 and 4.2

shows security certification and years of experience of security staffs within the critical infrastructures.



Graph 4.1 security certifications at critical Infrastructure

The survey shows that large portion of the security staff (74.6%) do not have any kind of security certifications. This shows that, even if security is very vital and a necessity, on job training whether national or international security training and certification is neglected. The increase and diversity of cyber threats, tremendous development in technology and complexity of cyber attacks, the preparedness and appropriate response can only be addressed by having well qualified security professionals within critical infrastructures. However its only 14.3% and 11.1% of the professionals surveyed do have a national and international security related certifications respectively. The next graph shows the years of experience of security staff at critical infrastructures.



Graph 4.2 Years of Experience

From the total population of security staff surveyed 98.4% have 2 years and above work experience within the critical infrastructure. This shows that they have ample experience concerning cyber security within the critical infrastructure. This also contributes to the validity and reliability of the survey findings.

4.3 Cyber Security Challenges at Critical Infrastructures

Critical Infrastructures are very vital for the proper functioning of a government and even for existence of a nation. Chee-wooi Ten (2010) stated the importance as critical infrastructures are complex physical and cyber based systems that form the lifeline of modern society, and their reliable and secure operation is of paramount importance to national security and economic vitality. In most sense, the cyber system forms the back bone of a nation's critical infrastructure, which means that a major security incident on cyber system could have significant impacts on the reliable and safe operations of physical systems rely on it (p.1).

Due to the importance of critical infrastructures, studying the challenges, identifying the security threats and taking appropriate measures are very important. Chee-wooi Ten(2010) emphasized this as due to the fast-growing intrusion attempts through cyber space , analysis of direct and indirect cyber vulnerabilities and cyber threats is important(p.2). Goetz (2002) stated that the analysis identifies the possible consequences and measures to prevent them from attacks (As Cited By Chee-wooi Ten, 2010, p.2).

Accordingly, this survey research targets to identify the challenges of cyber security at critical infrastructures on eight security threats namely,

- Lack of in-house expertise,
- Inadequate enabling technology,
- Insufficient funding,
- Evasion of existing preventive security controls,
- Difficulty in locating right security alert,
- Loss of sensitive or confidential data for non mobile resources,
- Loss of mobile devices containing sensitive or confidential data and,
- Poor leadership.

The respondents are asked to rate the above challenges of cyber security in a Lickert scale from 1 to 5 as 1: Strongly Disagree, 2: Disagree, 3: Undecided, 4: Agree and 5: Strongly Agree. The questionnaire is tested for reliability with 0.825 Cronbach's Alpha. The table4.4 shows the reliability testing on the above eight items.

Reliability Statistics

Cronbach's Alpha	N of Items
.825	8

Table 4.4 Reliability Statistics for eight questionnaire items on challenges of cyber security

To show the result of the survey, the findings on the challenges of cyber security at critical infrastructures are grouped in to four namely undecided, disagree, strongly disagree and the aggregate of agree and strongly agree.

The survey indicated that lack of in-house expertise (66.7%) is the top rated security challenge at the selected critical infrastructures. Cyber security, without expertise whether in-house or outsourced, is unthinkable. This survey shows that lack of in-house expertise is the top rated challenge at the selected critical infrastructures. Lack of in house expertise to ensure cyber security at critical infrastructure is main issue in Africa as a whole. Jensen(2001) confirms this as , "the availability of specialist training in telecommunications is currently extremely limited on the continent [Africa]" (As Cited in Kritzinger and Solms,2012,p.2).Moreover the interview with officer #1 confirmed this as:

> *"We have several challenges to secure cyber space. From these challenges lack of qualified experts and locating and acquiring appropriate technology are the most notable. Additionally compliance of internal users is a threat for cyber security."*

The second rated security challenges indicated by the respondents are inadequate enabling technology and difficulty in locating the right security alert (with equal percentile of 61.9%). There are several technologies for securing cyber space. United State General Accounting Office /GAO/ (2004) report states that many cyber security technologies that can be used to protect critical infrastructures from cyber attack are currently available, while other technologies are still being researched and developed. These technologies, including access control technologies, system integrity technologies, cryptography, audit and monitoring tools, and configuration management and assurance technologies, can help to protect information that is being processed, stored, and transmitted in the networked computer systems that are prevalent in critical infrastructures (Cybersecurity for Critical Infrastructure Protection, 2004, p.2).

To secure cyber space it is highly required to equip with technical aspects of cyber safety like up-to-date anti-virus packages and regularly patched operating systems. However this is not the case as identified by the survey. It is not only the case of Ethiopia however the African continent faced this challenge as well. In describing this Kritzinger and Solms (2012) in their research in titled "A Framework for Cyber Security in Africa" stated that the last problem focuses on the technical aspects of cyber safety. Cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched(p.3). The interview conducted with officer #2 stated the challenges of appropriate enabling cyber security technology as:

> *"Recently we have subscription of antivirus packages. However this is not a case all the time. We have also a problem in using appropriately patched operating system. This makes our system vulnerable for attack"*

The third rated security challenge is Evasion of Existing Preventive Security Controls (60.3%). Evasion of preventive security controls can emanate from company insiders /insider threats/, hackers, hacktivists, nation state attack or proxies and criminal groups. In stating the challenge of evasion of existing security controls officer #6 stated that:

> *"The main problem we observed as a security challenge in our organization is the improper use of credentials by our staff. For example, due to several reasons staffs are using other staff's credentials; password and user names to prepare bills and for financial operations. This evasion of security policy is the main security challenge".*

The IEEE computer security(2007) clearly stated the cyber threats coming from insider threats as in 1997 US Department of Defense (DoD) inspector General Report found that 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization(p.61). In addition to hackers and hacktivism, cybercrime and cyber breach is also perpetuated by organized crime groups and state and state affiliated proxies. Broadhurst et al.(2014) stated that today we find that numerous governments / or their proxies / are using internet technologies to commit crime. Therefore this finding, i.e. evasion of existing preventive security controls, is consistent with previous researches done in this area.

Additionally this survey indicated the fourth rated security challenges at critical infrastructures as insufficient funding and poor leadership (with equal percentile of 58.7%). Cyber security costs money, requires up-to-date technology, expertise and leadership. For instance countries are spending large sum of money for this effect. Briton and Watikins (2011) and Boulanin (2013) stated that through consolidated numbers are hard to come by, the amount of money spent on defense-related aspects of cyber security is rising (As Cited by Cavelty, 2014, p.2). United Kingdom, for instance spent large sum of money for cyber security. Minister for the Cabinet Office and Paymaster General (2011) stated that the United Kingdom/UK/ lists cyber security as a top priority and has committed 650 million pound over four years for transformative national cyber security programme (As cited By Niekerk and Solms, 2013, p.1). INSAs Critical Mass Cyber Security Requirement Standard (CMCSRS) (2017) stated that the top leadership should allocate

optimum resources and 0.5% of the organization's annual budget for cyber security (p.26). However officer #2 stated that:

> *"Even if we are in the process of implementing INSA's Cyber security standard, we still faced challenge of insufficient budget. The yearly budget allocated specifically for our unit is insufficient for acquiring the technologies we need and for capacity building for our staff. This is the other challenge in our unit".*

Additionally Ethiopia's CMCSRS (2017) stated that the top leadership should own the overall responsibility of cyber security of the organization and should be a model for the improvement of the cyber security (p.31). However as stated above insufficient funding and poor leadership are rated challenges. Therefore this requires a revisit of the standard and detail study on amount and usage of budget and the leadership's effectiveness and efficiency.

The last two rated security challenges are loss of sensitive or confidential data /non mobile resources/ (52.4%) and Loss of Mobile Devices Containing Sensitive/Confidential Data (44.4%). Loss of sensitive or confidential data from non mobile and mobile devices can affect the proper functioning at critical infrastructures. In describing the threats coming from mobile devices (Ciso, 2009) stated that "More individuals worldwide gain Internet access through mobile devices. Cyber criminals will have millions of inexperienced users to dupe with unsophisticated or well-worn scamming techniques that more savvy users grew wise to (or fell victim to) ages ago" (As Cited in Kritzinger and Solms,2012,p.2). In strengthen this Paul Ruggiero and Jon Foote (2011) stated that in more recent years, losing a smart phone or mobile devices can also jeopardize financial information stored on the device in banking and payment apps, as well as usernames and passwords used to access apps and online services(p.3). Similarly Ponemon institute study (2008) found that loss of labtops were top cause of data breaches representing 35% of the organization polled (As cited in White Paper: Enterprise Security Symantec, 2008,p.6).Therefore critical infrastructures should have well studied strategy and formulate a policy concerning mobile device usage in work environment.

The following table, table 4.5, shows the percentile distribution on each Lickert scale (1 to 5) on each cyber security challenges.

	Strongly Agree Plus Agree	Undecided	Disagree	Strongly Disagree
Lack of in-house Expertise	66.7	19	12.7	1.6
Inadequate Enabling Technology	61.9	15.9	17.5	4.8
Insufficient Funding	58.7	11.1	20.6	9.5
Evasion of Existing Preventive Security Controls	60.3	15.9	22.2	1.6
Difficulty in Locating Right security alert	61.9	15.9	20.6	1.6
Loss of Sensitive or confidential Data.(non mobile Resources)	52.4	23.8	17.5	6.3
Loss of Mobile Devices Containing Sensitive/Confidential Data	44.4	23.8	25.4	6.3
Poor Leadership	58.7	17.5	15.9	7.9

Table 4.5 Percentile Distribution of Cyber Security Challenges

In this survey human resources at critical infrastructures are surveyed from aspect of recruit, develop and retain talent within the organization. The reliability of the questionnaire on these three questionnaire items related to recruit, develop and retail is 0.875 Cronbach's Alpha which is reasonably high. From total of the respondents surveyed 60.3 % indicated that critical infrastructures are inadequately prepared to recruit talent from the existing market. In strengthening this officer #2 stated that:

> *"In recruiting IT security staffs we are strictly using the procedures set by human resource. However the screening and evaluation in recruitment is our main challenge. Sometimes the educational document fails to show the exact capability of the candidate".*

The survey also indicated that 63.5 % of the respondents believe that critical infrastructures are inadequately prepared to develop talent within the critical infrastructures. Officer #2 stated that:

> *"Due to budgetary limitations it is difficult to engage in full fledge capability building training for all staff at national or at international level. We have limited amount of training budget specifically for security. But we are working to change this."*

Finally 63.5% of the respondents indicated that critical infrastructures are inadequately prepared to retain talent within the organization.

The interview conducted with Officer #2 stated this as:

> *"There is high staff turnover. We have a difficulty in retaining staff. One of the reasons for this is insufficient benefits. We are trying to address this issue. The other reason is the competition from other sectors for IT professional."*

Therefore critical infrastructures are inadequately prepared to recruit, develop and retain talent. This result is consistent with the first challenges of critical infrastructures which is lack of in-house expertise.

4.4 Trends of Growth in Cyber Security Threats

Cyber security threats are increasing from time to time. The effect and the cost of cyber security breaches on organizations or critical infrastructures are very high. Cavelty (2014) stated that in recent years , a number of sophisticated cyber-attacks and intensifying media attention have combined to give the impression that cyber-incidents are becoming more frequent , more organized , more costly , and altogether more dangerous (p.2). Critical infrastructures should be in a position to protect their IT infrastructures from security breach.

One of the foundations for cyber security protection is to find the security threats and works towards eliminating or minimizing the effect and cost of security breach. Critical infrastructures should identify recent security threats and formulate a strategy and practices to eliminate or minimize the possibility of that security threat.

Accordingly this research identified the growth trends of six cyber security threats namely

- Mobile computing,
- Employee's mobile Devices or Applications/Bring Your Own devices or Applications/BYOD or BYOA//,
- Attacks via E-mail,
- New Application Implementation or App Development Process,
- Attacks via Social Media and,

- Nation on a Nation Breach.

The data is collected from the respondents on the above security threats using Lickert scale that is 1: Strongly Disagree, 2: Disagree, 3: Undecided 4: Agree and 5: Strongly Agree. The questionnaire is tested for reliability with Cronbach's Alpha of 0.742 for the above six items.

From the total respondents 74.6% indicated that there is a growth of cyber security attacks via E-mail. Due to the increase in number of users of internet services, cyber security threats from E-mail service obviously increased. In strengthening this officer #4 stated that:

> *"E-mail is one of the services targeted by hackers in forms of social engineering attacks. They send different messages and malicious codes which trick the users for their advantage. These threats are growing even with mobile network. The lack and the limited awareness of end users make this threat more dangerous than it actually is".*

Rowe et al. (2010) describe the increase in number of users of internet services and the threats associated in Africa as broad band services are opening in the continent, which means more users would be able to access the web, translating into more viruses and spam from online (As Cited in Kritzinger and Solms, 2012, p.1).In strengthening this Sophos (2009) stated that 89.7% of all business Email is spam. Similarly the selected critical infrastructures of this study indicated that attack via email is growing considerably.

In this survey, 68.3% of the respondents indicated that there is a growth of cyber security threat using Mobile computing. Officer #4 stated the increase of cyber security threats in mobile computing as:

> *"Recently mobile computing is increasing in our country. Employees are using their mobile devices to connect wireless networks outside the organization and within the organization. Due to this intruders are using this as a medium of attack."*

In describing the growth of cyber security threats in Africa Rowe et al. (2010) paint a frightening picture about the level of cyber security threats in Africa continent as a whole. They argue that "about 80% of PCs in African continent are already infected with viruses and other

malicious software's" (As Cited in Kritzinger and Solms, 2012, p.2). It is not only the cyber security threat from personal computers that shows a grim picture in Africa but mobile computing. In strengthening the cyber threats of mobile computing Kritzinger and Solms (2012) stated that while this picture alone is very threatening , it is further alarming to note that it is not only personal computers that are affected in Africa as whole. But cyber crime is exploiting mobile devices in Africa too (p.2).

From the total respondents 63.5 % indicated that an attack via social media is growing. Nowadays social networking users are increasing in Africa. In describing the increase in number of users and the Cybersecurity threats in Africa, Kritzinger and Solms(2012) stated that the rapid leap of using ICTs and broad band opens a gap for a number of cyber threats that can result in cyber crime (p.1). Shaabi and Gharibi (2010) stated that nowadays, millions of internet users regularly visit thousands of social websites to keep linking with their friends, share their thoughts, photos, videos and discuss even about their daily-life (p.1). The same scholars stated clearly the security threats of these technologies as the internet today, unfortunately, offers to the cyber criminals many chances to hack accounts on social network sites and the number of malicious programs that target the social websites is very huge (Shaabi and Gharibi, 2010, p, 2). In strengthening this officer #4 stated that:

> *"Our staffs are using the social networking sites using our cooperate network which makes our security vulnerable for attacks. We prepared a policy to reverse this. However enforcement of this policy is a challenge. Due to the number of users of social networking sites especially Facebook, the threat from this service is growing".*

Similarly CISCO (2009) stated that social networking sites are the target for cyber criminals as three million computers have been infected with koobface. Therefore the finding in this research is consistent with the previous research done in this area.

In addition 58.7 % the respondents of this survey indicated that cyber security attacks are due to new App implementation or App Development. 55.6% of the respondents indicated that attacks from Employee's mobile devices or application/BYOD or BYOA/ is on growing trend. In

describing the security threats from user's devices, Kritizinger and Solms (2012) stated that the worst part of it all perhaps is that many of these users, sadly, do not have a clue as to how to protect themselves and their personal information against the cyber attacks directed at their gadgets (p.1). This in turn creates a threat for critical infrastructures as identified in this survey.

The interview conducted with Officer #1 describes the growth of cyber security threats as:

> *"Cyber threats are growing mainly from E-mail service, social media, and hacktivist attacks. But due to the stand alone systems and the old IBM technology we are using for billing and finance, the effect of these threats are limited. However we are in the process of adapting new technology. Therefore the cyber security growth threats really concerned us."*

Finally Nation on nation attack is the other cyber security threat in this globalized world. From the total respondents of the survey 41.3% indicated that nation on nation cyber attack is growing. In explaining nation on nation attack Cavelty (2014) stated that cyber space , unlike the air , space, or the sea , is entirely man-made realm , at all times shaped by economic and political forces(p.2). The recent phenomenon reported on international media on October 11, 2017 state sponsored cyber security breach by North Korea hackers stole US-South Korea war plans and 235 Giga bytes worth of military data. This shows that nation on nation attack using cyber space is possible and it is on growing trend. In strengthening this officer #2 stated that:

> *"In this globalized world the effect of computer network specifically the internet makes the growth of cyber threats coming from one nation on the other is increasing. Possibly Ethiopia might be affected in the future"*

Therefore critical infrastructures should be prepared for this attack and minimize its effect on social, economic and political realm.

4.5 Preparedness to Cyber Security Threats at Critical Infrastructures

Cyber security threats and cyber breach are increasing from time to time. It has huge cost and affects the reputation of organization and customer trust. Due to this NIST framework of 2017 stated that cyber security threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy and public safety and health at risk. Similar to financial and reputational risk, cyber security risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers (p.5).Specifically cyber security breach at critical infrastructures can affect the well being of citizens and the proper functioning of a government. Any nation whether developed or developing should be in a position to protect its information infrastructure at its critical infrastructure. One of the foundations for this protection is to thorough study of the capabilities of critical infrastructures on how to detect, prevent and respond to cyber security threat and cyber breach.

In this survey the readiness and preparedness at critical infrastructure is accessed from the view point of seven cyber security threats namely insider attacks , criminal threats , attacks via email, nation state attacks, hacktivist attacks , attacks via social media and executive branch response. The questionnaire six items are tested for reliability with a Cronbach's Alpha of 0.942 which is considerably high. The respondents indicated that the capability of critical infrastructures on these cyber security threats on the three technical sub pillars namely detect , prevent and respond by using Lickert scale from 1 to 5 that is 1: inadequately prepared, 2: somewhat inadequately prepared , 3: somewhat prepared , 4:well prepared, and 5: extremely well prepared.

4.5.1 Preparedness to Detect Cyber Security Threats

According to National Institute of Standards and Technology /NIST/ (2017) detect function refers to developing and implementing the appropriate activities to identify the occurrence of cyber security event (Framework for improving critical Infrastructures Cyber Security Version 1.1, p.12). This study measures preparedness to detect cyber security threat at critical infrastructures. The result of the respondents is categorized in to three as aggregate of

inadequately prepared and somewhat inadequately prepared, somewhat prepared, aggregate of well prepared and extremely well prepared.

The survey indicated that critical infrastructures inadequately prepared to detect Nation State Attacks (61.9%) and attacks via Email (61.9%). As it is discussed above security threats, nation state attack and attack via email, is on growing trend at the selected critical infrastructures. The inadequacy to detect these attacks highly affects the proper functioning of critical infrastructures. The effect of nation state attack, for instance Estonian cyber attack in 2017, highly affects the social, economy and the political environment of the country(Stephen Herzong,2011,pp1-3). The same holds to true for attacks via Email using malicious codes or social engineering attacks.

Significant number of respondents (60.3%) indicated that critical infrastructures are inadequately prepared to detect Hacktivist Threat, attacks via Social Media and criminal Threats. Due to the vast number of users of social Media and Email services, this result indicated that there is high probability that these security threats can impact critical infrastructures. Similarly Herzog (2011) stated that Hacktivist posses the ability to disrupt or destroy government operations, banking transactions, city power grids, and even military weapon systems (p.1). In strengthening this officer #4 stated that:

> *"Activists are strongly using social Medias to promote their agendas and disrupt services for their objective. This trend of cyber security threat is growing in Ethiopia."*

Officer #4 further stated that:

> *"Due to the limitation of appropriate technology, lack of qualified experts and staff negligence to detect cyber threats, we are facing a challenge to detect and take appropriate measures.*

The details of the respondents are shown in the following table.

Cyber Security Threats	Aggregate of Inadequately Prepared & Somewhat inadequately Prepared (%)	Somewhat Prepared (%)	Aggregate of Well Prepared & Extremely Well Prepared (%)
Nation State Attacks	61.9	17.5	20.6
Attacks Via E-mail	61.9	17.5	20.6
Hacktivist Threat	60.3	17.5	22.2
Attacks Via Social Media	60.3	15.9	23.8
Criminal Threats	60.3	20.6	19.0
Insider attacks	58.7	11.1	30.2

Table 4.6 Percentile Distribution of Level of Preparedness to Detect Cyber Security Threats

The above result from the respondents indicated that the critical infrastructures "inadequately and somewhat inadequately prepared" to detect all the six cyber security threats.

4.5.2 Preparedness to Prevent Cyber Security Threats

Prevention or Protection of any cyber security breach is the ultimate goal of any critical infrastructure. According to NIST framework for improving critical infrastructures cyber security (2017) prevent refers to developing and implementing the appropriate safeguards to ensure delivery of Critical Infrastructures (p.12).However complete prevention of security threat is nearly impossible in these days. But organizations capability to prevent cyber security threat should be increased which in turn saves money and organizations reputation. Therefore critical infrastructures should have higher capability to prevent cyber security threats. However the survey indicated that critical infrastructures are inadequately prepared and somewhat inadequately prepared for the six cyber security threats and for executive branch response.

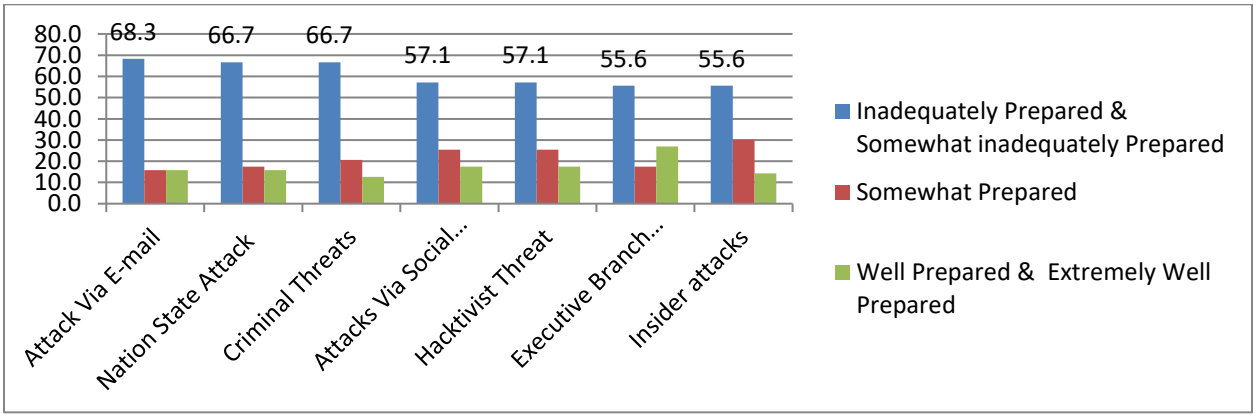
The questionnaire is tested for reliability on the seven items used to collect data on prevent sub pillar with the Cronbach's Alpha of 0.946. The respondents specifically indicated that critical infrastructures are inadequately prepared to prevent for attacks via Email (68.3%), Nation State Attacks (66.7%) and Criminal threats (66.7%). Officer #5 stated that:

"Due to the lack of appropriate technology to prevent cyber attacks like attacks via e-mail is difficult to prevent. Moreover negligence of the staff is a major threat in our institution"

Moreover the survey shows that critical infrastructures are inadequately prepared to prevent attacks via Social Media (57.1%), Hacktivists threats (57.1%), Executive Branch response (55.6%), and insider threats (55.6%). In summarizing the inadequacy to prevent cyber attacks, officer #5 stated that:

"We have a difficulty in performing over all system testing and auditing periodically. This is one of the causes for cyber threats."

Therefore the prevention sub pillar from cyber security threat requires due attention at critical infrastructures. The graph below shows the details.



Graph 4.3 Level of Preparedness to Prevent Cyber Security Threats

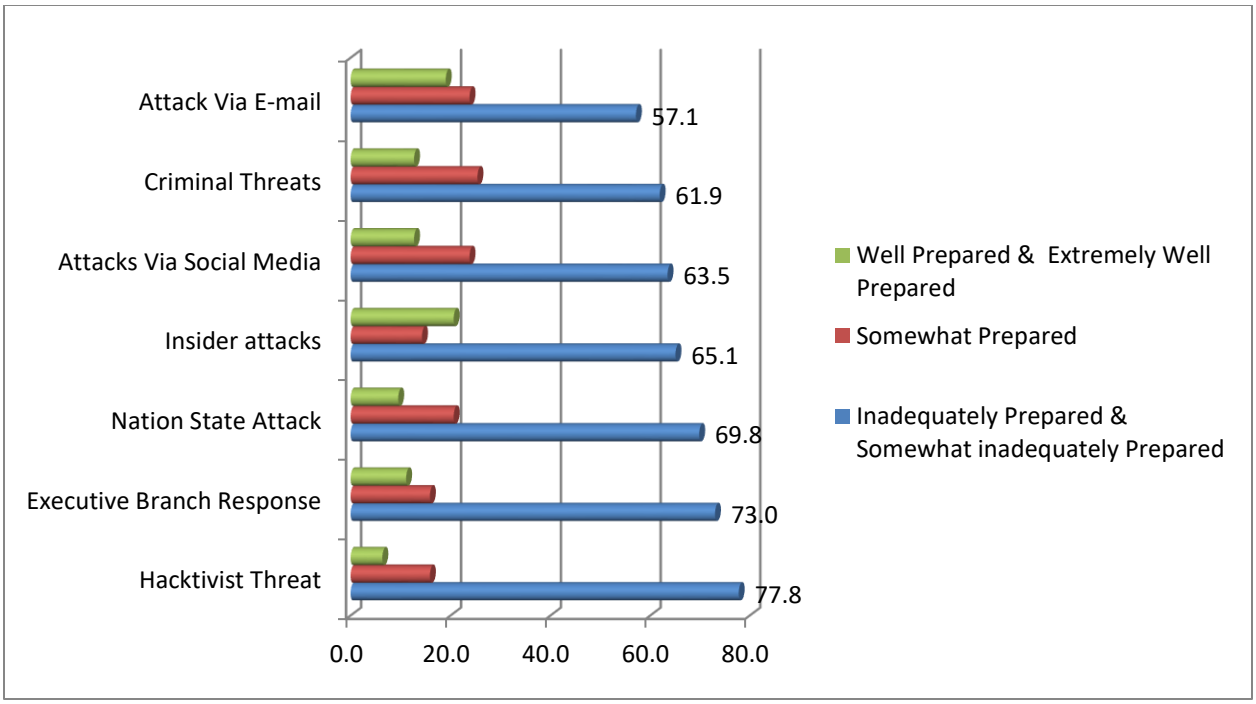
4.5.3 Preparedness to Respond to Cyber Security Breach

Efficient and effective response to cyber security breaches save money, minimize the effect on company reputation and customers' dissatisfaction. NIST (2017) framework defines respond as a function of developing and implementing the appropriate activities to take actions regarding detected cyber security event (p.13). Appropriate and timely response for cyber breach should be given due emphasis at critical infrastructures. This is because proper response to cyber security breach of any kind can minimize the devastating effect at critical infrastructures. However the survey indicated that critical infrastructures are inadequately prepared or somewhat inadequately prepared for all six cyber security attacks and executive branch response.

From the total respondents 77.8% indicated that critical infrastructures are inadequately prepared to respond to hacktivist threats. As it is discussed above the inability to respond to hacktivist threats in a timely and appropriate way can create social, economic and political instability. Because hacktivism falls in to the grey area between politics and crime, most closely resembling what is traditionally understood as subversion-"the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order" (Kosina, 2012, P.22).

Considerable number of respondents (73.0%) of the survey further indicated that executive branch of critical infrastructures are inadequately prepared to respond for cyber breaches. Even if the Ethiopian cyber security Standard, i.e Critical Mass Cyber security Requirement Standard (CMCSRS) of 2017, stated that the top leadership should own the overall responsibility of cyber security this survey indicated that the top branch of management is inadequately prepared to respond to cyber security attacks.

In addition 69.8% and 65.1 % of the respondents indicated that critical infrastructures are inadequately prepared for nation state attacks and insider attacks respectively. Moreover critical infrastructures are inadequately prepared for attacks via social media (63.5%), criminal threats (61.9%) and attack via Email (57.1%). The details are shown in the graph below.

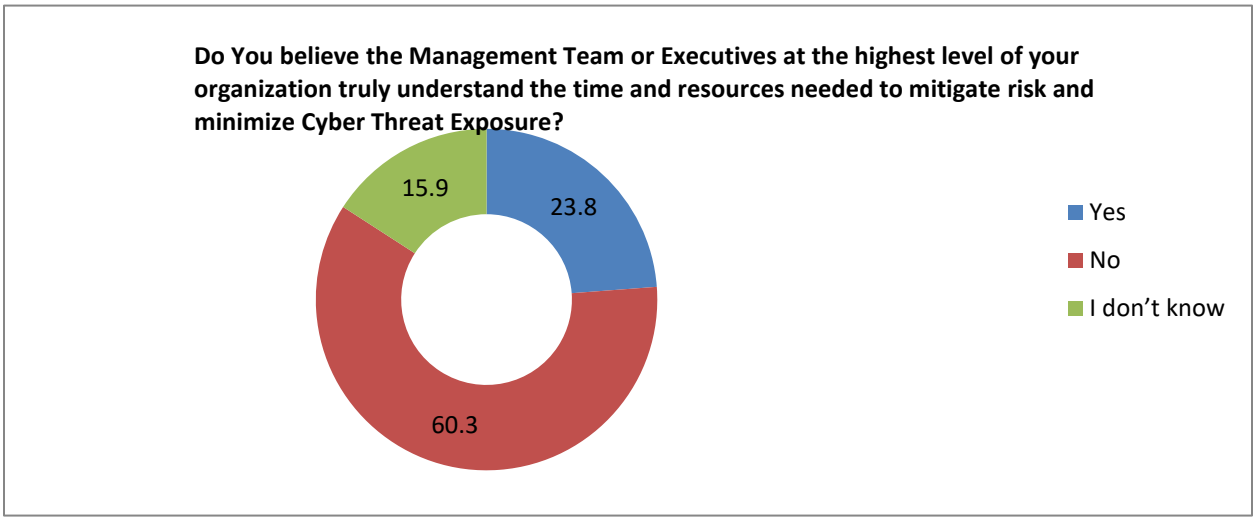


Graph 4.4 Level of Preparedness to Respond Cyber Security Threats

On average 66.9% of the respondents indicated that critical infrastructures are inadequately prepared to respond for six cyber security threats and for executive branch response. Specifically this survey shows that executive branch of the critical infrastructures are inadequately prepared to deal with cyber security breach. On all the three technical sub pillars , detect , prevent, and respond to cyber security threats and breaches , the respondents indicated that critical infrastructures are inadequately prepared for hacktivist threats(65.1%) , attacks via social media (64.6%), nation state attacks (66.1%) , insider attacks(59.8%), criminal threats(63.0%) and attacks via Email(62.4%).

This shows that critical infrastructures are inadequately prepared to detect, prevent and respond to cyber attacks and breaches. Moreover the executive branches are inadequately prepared to prevent and respond to cyber breaches. Furthermore in this survey the respondents are asked to indicate their belief as “Yes , No or I don’t Know “ whether the management team or executives at the highest level of their organization truly understand the time and resources needed to mitigate risk and minimize cyber threat or exposure. 60.3% of the respondents indicated their belief that the highest level of the organizations lacks the understanding concerning the time and

resources needed to mitigate and minimize cyber threat exposure. The details are shown in a pie chart below.



Graph 4.5 Management Team or executives understanding towards Cyber Security

4.6 Discussion

As it is stated in chapter three, Research Methodology, this research targets to answer three research questions based on International Telecommunication Union's /ITU/ pillars namely Legal, Technical, and Capability Building. As it is discussed previously the technical pillar of this research is merged with NIST framework to improve critical infrastructures draft version 1.1 core technical processes identify, detect, prevent, respond and recover cyber threats and breaches.

The first research question of this survey is to identify the challenges of ensuring safe cyber space at selected critical infrastructures. Critical infrastructures are the corner stone's for the existence of a nation. In strengthening this GAO (2004) report of United State describe critical infrastructures include those assets, systems, and functions vital to our national security, economic need, or national public health and safety. Critical infrastructures encompass a number of sectors, including many basic necessities of our daily lives, such as food, water, public health, emergency services, energy, transportation, information technology and telecommunications, banking and finance, and postal services and shipping(Cybersecurity for Critical Infrastructure

Protection, 2004,p.11).Ensuring cyber security of IT infrastructure at critical governmental and private organizations is very vital for proper functioning of a nation. Hence critical infrastructures cyber security should be examined, challenges they have should be pin pointed and solutions must be formulated.

Accordingly this survey research which is a case study of three critical infrastructures' in Ethiopia identified major challenges. This study indicated that critical infrastructures face challenges of lack of in-house expertise, difficulty in locating the right security alert, inadequate enabling technology and evasion of existing security controls.

Cyber security requires expertise or trained professionals. GOA (2007) report states that Technologies do not work in isolation. Cybersecurity solutions make use of people, process, and technology. Cybersecurity technology must work within an overall security process and be used by trained personnel (Cybersecurity for Critical Infrastructure Protection, 2004, p.21). Therefore critical infrastructures in Ethiopia should develop a strategy to recruit, develop and retain expertise. The other main component for cyber security is technology. Cyber security enabling and alerting technologies should be available. In strengthening this, GOA (2007) report of US stated that the federal government could lead to the development and availability of more cyber security technology products and can take long-term actions to increase the quality and availability of cyber security technologies available in the marketplace(Cybersecurity for Critical Infrastructure Protection, 2004, p.20).

Additionally this survey research identified further cyber security challenges namely insufficient funding, poor leadership, loss of sensitive or confidential data from non mobile and mobile devices. Cyber security requires sufficient amount of funding and leadership. Cyber security technology costs money. Critical infrastructures should acquire these cyber security technologies. GOA (2007) report states that there is a variety of technologies that can be used in support of cyber security. Some technologies, such as firewalls and biometrics, help to protect computers and networks against attacks, while others, such as intrusion detection systems and continuity of operations tools, help to detect and respond to cyber attacks in progress (Cybersecurity for Critical Infrastructure Protection, 2004, p.26).As it is discussed above nations

cyber security spending is increasing from time to time. However, proper utilization of these resources requires leadership. Therefore critical infrastructure in Ethiopia should develop mechanize to overcome these challenges.

The survey also indicated growing threats of cyber security. The survey indicated that attack via E-mail, mobile computing and attacks via social media are the top growing cyber security challenges at critical infrastructures. As it is discussed above broad band connectivity is growing in Africa. More and more people are using internet services using mobile devices. This survey indicated that these threats are growing. Ruggiero and Foote (2011) stated the security challenges coming from E-mail, mobile computing and social networking as Smart phones and personal digital assistants (PDAs) give users mobile access to email, the internet, GPS navigation, and many other applications. However, smart phone security has not kept pace with traditional computer security. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on personal computers (p.1). Therefore critical infrastructure should formulate a policy and enforce use of mobile device, Personal E-mail and social networking sites using cooperate network infrastructures.

This study also indicated that cyber security challenges coming from new App implementation and development and nation on nation breach are on growing trend. Herzog (2011) stated the increase cyber threat on nations as increased communication, networking, and reliance on digital infrastructure in the information age empower transnational resistance movements and create new vulnerabilities for nation-states. Even if the benefits of the information age are numerous, but nascent threats like transnational cyber terrorism and information warfare exist alongside the positive aspects of globalization (p.5).

Finally this research indicated that selected critical infrastructures are inadequately prepared to detect, prevent and respond to nation state attack, attack via e-mail , hacktivist threat , attack via social media , criminal threats and insider threats. This shows that critical infrastructures are vulnerable for cyber attacks from any of these threats. This creates a tangible danger for the

nation. In explaining the dangers of cyber threats and breaches of Estonia, Herzog (2011) stated that the severity of the Estonian cyber attacks served as a wake-up call to the world, as it became clear that potentially autonomous transnational networks—like unhappy pro-Kremlin "hacktivists"—could avenge their grievances by digitally targeting and nearly crippling the critical infrastructure of technically sophisticated nation-states (p.10).

The second research question of this thesis is to identify the practices and processes of cyber security at selected critical infrastructure in Ethiopia. Cyber security practices and processes are guided by handful of legislations, directives, policies and standards. In the proceeding portion, these legislations, directives, policies and standards are discussed and related with what existed at selected critical infrastructures.

4.7 Cyber Security Practices: Legislations, Policies, Institution and Standard

The legal framework for securing critical infrastructures includes handful of legislations which extends from Telecom Fraud offence to establishment of a central organ to deal with cyber security. This central body, Information Network Security Agency/INSA/, is established in 2006 with council of ministers regulation No. 130/2006.The regulation No. 130/2006 stated that the objective of the agency is to ensure the country's use of information and information communication network technologies and telecommunication in the implementation of its peace, democratization and development programs is without risk to the national security. Since its establishment in 2006, there are three consecutive re-establishment legislations in 2011, 2013 and 2014. These council of ministers regulations are council of Ministers Regulation No. 250/2011, 808/2013 and 320/2014. These three legislations provide vast power to INSA in order to secure critical infrastructures.

Moreover the Ethiopian government in recognizing the inadequacy of the former penal law issued a proclamation on Telecom Fraud Offence with Proclamation No. 716/2012. Furthermore there are two policy issues which are related with ensuring safe cyber space. These are National Spatial Information Technology Policy and the National Information and Communication Technology Policy and Strategy.

Hevneret al.(2004) stated that information systems are implemented within an organization for the purpose of improving the effectiveness and efficiency of that organization (p.76). Accordingly INSA issued cyber security enforcement standard called Critical Mass Cyber Security Requirement Standard/CMCSRS/Version 1.0 in September 2017. The main objective of this standard is to secure the critical information and information systems of the country in order to protect national interest (CMCSRS version 1.0, 2017, p.14).

The CMCSRS version 1.0(2017) stated that the standard enables organizations to create significant and unstoppable cyber security capability and process , i.e. a 'Critical Mass ' of cyber security , which will continuously build cyber security capabilities and establish cyber security processes in order to effectively manage their cyber security(p.8). Even if this is the intention of the CMCSRS version 1.0 of 2017, the interview conducted with the Officer #3 clearly stated the challenges as:

> *"Even if Critical Mass was issued in 2017, we are still in the process of implementing it at critical infrastructures. There are several challenges that range from staff capability to resistance of change. But I believe that we are on the right track"*

The CMCSRS of 2017 contains Model, Framework, Architecture and content. The standard contains a cyber security strategic management model to express the concepts of the critical mass cyber security standard. These are presented using three dimensions namely,

- **Perspective Dimension** (D1) which includes capability building, process, and stake holders and mission perspectives of cyber security. The capability building includes leadership, governance, management, human resource and technology (CMCSRS version 1.0, 2017, p.17).However this research identified Lack of in-house expertise, Inadequate enabling technology and difficulty in locating the right security alert are the main challenges at critical infrastructures in Ethiopia. The survey also indicates that critical infrastructures are inadequately prepared to recruit, develop and retain human resource within their organization. The respondents also indicated that the executives or higher level management is inadequately prepared to deal with cyber security incident. This shows that the perspective dimensions requires due attention at critical infrastructures. Officer #2 explained these as :

"Capability building is the sole responsibility of the respective organizations. Capability building for leadership and expertise are implemented based on their gaps. Therefore the organizations should identify these and prepare and implement capability building based on their own in-house framework."

It is not only the capability building but also the technical pillars that is prevent, detect and respond shows a grim picture at critical infrastructures. This survey research identified that critical infrastructures are inadequately prepared to prevent, detect and respond to cyber security threats and breaches. Concerning these, Officer #3 responded that:

"The critical mass only presents the strategic view of the cyber security processes. The implementation to detect, prevent and respond mainly deals with technical issues. I believe that there are concrete problems on the ground."

- **Level Dimension (D2).** This dimension contains strategic, Tactical and operational levels of cyber security. Capability building, processes, stakeholders and mission have these three levels. (CMCSRS version 1.0, 2017, p.17).
- ,and the last dimension is **Analysis Dimension(D3).**This dimension is applied to analysis cyber security at strategic , tactical and operational levels of capability building , processes , stake holders and mission (CMCSRS version 1.0,2017,p.17).

This CMCSRS version 1.0 contains mandatory requirements, absolute prohibition, and highly recommended, not recommended and truly optional activities. This standard will be updated periodically. In Explaining these Officer #3 stated that:

"Even if it is only a year and half since the release of the critical mass we are engaged in implementing and collecting feedback from organizations which help us for further update of the critical mass."

This standard is a game changer which enables organizations to change different aspects of their cyber security such as their awareness and culture, human capability, structure and processes , organization should also identify 80-20 in each area and focus on the 20% , based on the 80-20

rule(Pareto Principle) (CMCSRS version 1.0,2017,p.17). Accordingly, this research identified the challenges of cyber security at critical infrastructure and proposes a tailored cyber security framework based on CMCSRS version 1.0 and NIST framework for improving critical infrastructure cyber security.

4.8 Chapter Summary

This chapter presented the findings, analysis and discussion. This study indicated that critical infrastructures face challenges of lack of in-house expertise, difficulty in locating the right security alert, inadequate enabling technology and evasion of existing security controls. Additionally this survey research identified further cyber security challenges namely insufficient funding, poor leadership, loss of sensitive or confidential data from non mobile and mobile devices.

The survey also indicated growing threats of cyber security. The survey indicated that attack via E-mail, mobile computing and attacks via social media are the top growing cyber security challenges at critical infrastructures. This study also indicated that cyber security challenges coming from new App implementation and development and nation on nation breach are on growing trend.

Finally this research indicated that selected critical infrastructures are inadequately prepared to detect, prevent and respond to nation state attack, attack via e-mail , hacktivist threat , attack via social media , criminal threats and insider threats. This research also identifies the practices and processes of cyber security at selected critical infrastructure in Ethiopia. Cyber security practices and processes are guided by handful of legislations, directives, policies and standards.

CHAPTER SIX

The Tailored Cyber Security Framework for Critical Infrastructures

5.1 Overview

This study indicated several existing and future cyber security challenges at critical infrastructures. The challenges to enforce cyber security at critical infrastructures can be categorized in to four. These are:

1. Existing cyber security technological challenges,
2. Trends in growth of cyber security threats,
3. Existing challenges and level of preparedness to detect, prevent, and respond cyber security threats and breaches, and
4. Challenges to recruit, retain, and develop human resources.

As it is discussed in the findings, this research identified several challenges that exist at selected critical infrastructures. These challenges are lack of in-house expertise, inadequate enabling technology, evasion of preventive security controls, poor leadership, insufficient funding, difficulty in locating right security alert, and loss of sensitive or confidential data from mobile or non mobile resources.

This study also identified the growing challenges in securing different security threats. The study clearly shows that attacks via Email, mobile computing and attacks via social media are the growing security challenges at critical infrastructures. Moreover the findings of this study indicated that critical infrastructures faced challenges to detect, prevent, and respond to security threats and breaches. The study also shows that critical infrastructures are not adequately prepared to detect, prevent, and respond to Hacktivist threats, nation state attacks, insider attacks and attacks via social media.

Furthermore the study indicated that critical infrastructures executive teams at highest level of management within the organizations are not adequately prepared to respond to cyber threats or

exposures. Additionally critical infrastructures are inadequately prepared to recruit, develop, and retain human resources.

Cyber security challenge and inadequacy in processes can be solved by designing an IT artifact. Accordingly Hevner et al. (2004) stated that knowledge and understanding of a problem and its solution can be achieved in the building and application of the designed artifact (p.75). Due to this and to alleviate the above four categories of challenges a strategic level framework should be tailored based on NIST framework to improve critical infrastructures cyber security version 1.1 with a combination of INSA's Critical Mass Cyber Security Requirement Standard Version 1.0.

Kiriwandenyia et al. (2013) stated that a framework is a model artifact that provides a broader overview or skeleton of interlinked items which helps as a guide to achieve a specific objective. According to Hevneret al.(2004) IT artifacts are broadly defined as constructs (vocabulary and symbols), models(abstractions and representations) , methods(algorithms and practices), and instantiations(implemented and prototype systems).

Accordingly in this research attempts are made to tailor and propose an IT artifact specifically model or a framework based on:

1. The findings of this research. The challenges, the level of preparedness to cyber threats and the practices of cyber security at critical infrastructures are used as an input to develop the model. Accordingly Hevner et al. (2004) argue that truth and utility are inseparable. Truth informs design and utility informs theory (p.78).
2. INSA's Critical Mass Cyber Security Requirement Standard Version 1.0 ,and
3. NIST framework for improving critical infrastructure cyber security version 1.1.

Alter (2003), Bunge (1985) and Simon (1996) stated that information systems and the organization they support are complex, artificial, and purposefully designed. They are composed of people, structures, technologies, and work systems (As Cited by Hevner et al.; 2004; p.78). Accordingly the proposed artifact or framework for critical infrastructures contains people, structure and technologies as pillars. Walls et al. (1992) stated that design is both a process (set of activities) and a product (artifact) (As cited by Hevner et al.,2004,p.78). Moreover

Hevner(2004) stated that design describe the world as acted upon(processes) and the world as sensed(artifacts) (p.78).

Accordingly the proposed framework in this research contains processes of cyber security at critical infrastructures. March and Smith (1995) identify two design processes and four design artifacts. The two processes are build and evaluate. The artifacts are constructs, models, methods and instantiations (As cited by Hevner et al., 2004, p.78). Accordingly, this research includes the two design process, builds and evaluates and develop an artifact Model or a framework.

Designing an IT artifact like a model or framework is not a random process. Due to this Hevner et al. (2004) prepared seven guidelines in the building and application of an artifact (p.82). Accordingly in this research, the seven guide lines are considered and followed in tailoring the cyber security framework for critical infrastructures. The table 5.1 below shows Hevner et al. (2004) design research guide line which is used in this research for the proposed framework.

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Table 5.1 Design Research Guide Line

Different researchers design models or frameworks in different ways. For instance Desisa and Beshah (2014) developed an internet banking security framework for Ethiopian banking

industry. Based on the previous study conducted, the researchers identified the clients / customers/ to be the weakest link in the chain of security (p.2). Their framework recommended holistic multi-layered security that stretches towards client's side security and national financial and security intelligence and team incorporated (p.1).They stated that concepts learned from literature review and survey result, particularly from interview, leads to propose frameworks that realize holistic approach of internet banking security for Ethiopian banking industry (p.4).

Dlamini ,Taute and Radebe(2011) developed a high-level African cyber security policy as well as an African cyber security awareness framework to guide cyber security agencies , standards and legislation as well as specific initiatives to promote cyber security awareness. This is achieved through analysis of few cyber security policies from developed countries(USA, UK, Estonia, Korea) , identification of African countries that have such policies in place, and identification of the agencies , forums , workshops , conferences , organizations and other initiatives that are currently dealing with ICT and Cyber security policy and awareness in Africa including ITU, AfriNIC, ISG-Africa and country- specific organizations such as computer security incident response team(p.1).

Islam (2013) has developed framework for E-learning simply by identifying the major challenges and proposing corresponding solutions for each challenge. Krizinger and Solms(2012) in their article 'A Framework for Cyber Security in Africa' proposed comprehensive framework for Cyber safety based on four major cyber safety concerns in Africa discussed in recent literatures (p.1). These researchers identified four major cyber security problems in Africa namely lack of focused research in cyber security , lack of a proper integrated framework on legal and policy aspects , lack of cyber security awareness and regulation and lack of technical measure. The researchers further developed solutions for these problems and propose a comprehensive framework for cyber safety.

Similarly this research use the challenges and their forecast or growth identified at critical infrastructure in order to tailor cyber security framework for processes based on CMCSRS version 1.0 and NIST framework to improve critical infrastructure cyber security version 1.1.

Additionally interviews and extensive literature review are used as an input to tailor the cyber security framework.

The combination of these two standards provides the opportunity to follow INSA's Standard of 80-20 rule (Pareto Principle) (which states an organization should also identify 80-20 in each area and focus on the 20%) (CMCSRS version 1.0, 2017, p.17) and facilitate cooperation with international cyber security institutions.

As stated previously information systems are composed of people, structures, technologies and work systems. As a framework is an artifact of information systems they are also composed of these components. Accordingly the tailored framework contains the following main components:

- Organizations /Stake holders/: the two organizations involved in the process of cyber security at critical infrastructures are Cyber security Unit within the organization and INSA.
- Bags of Existing and growing threats
- NIST core processes
- CMCSRS OPDCA Process Cycle
- Key Indicators and Feedback.

3.2 Cyber Security Units and INSA

Cyber security units within the critical infrastructures with coordination and collaboration of INSA should prepare a bag of existing and growing security threats periodically. They should work towards implementing and enforcing the CMCSRS version 1.0. Additionally the collaboration extends to evaluating the success and failure of the processes.

3.3 Bags of Existing and Growing Threats

Williams et al. (2016) in their research of future scenarios and challenges for security and privacy reviewed the works of several researchers in relation to their topic. William et al. (2016) constructed future scenarios. Some of these are:

- Growth of the internet of things /IoTs/,
- Proliferation of offensive tools,
- Privacy becomes reinterpreted,

- Repressive enforcement on online order
- Traditional business models under pressure,
- Big data enables greater control, and
- Growth of public – private partnership (p.2).

Similarly INSA and cyber security units at critical infrastructures should construct bags of scenarios for existing, growing and future cyber security threats. These scenarios enable to focus and re-direct effort based on the likely hood of an events occurrence. Based on the likely hood of a threat at critical infrastructures, the security threat/s should be moved to or removed from a bag of growing threats. These bags of threats should be implemented at each function of NIST core processes. NIST core processes and bags of growing and existing security threats help cyber security activities to focus on immediate and potential threats separately.

Finally this tailored cyber security framework added only two main processes in the existing standard of INSA. These are concepts of existing and growing threats bag and NIST framework five processes namely Identify, Detect, Prevent, Respond, and Recover.

Graphical Representation of the Tailored Framework for Technical Processes of Cyber Security is presented in figure 5.1.

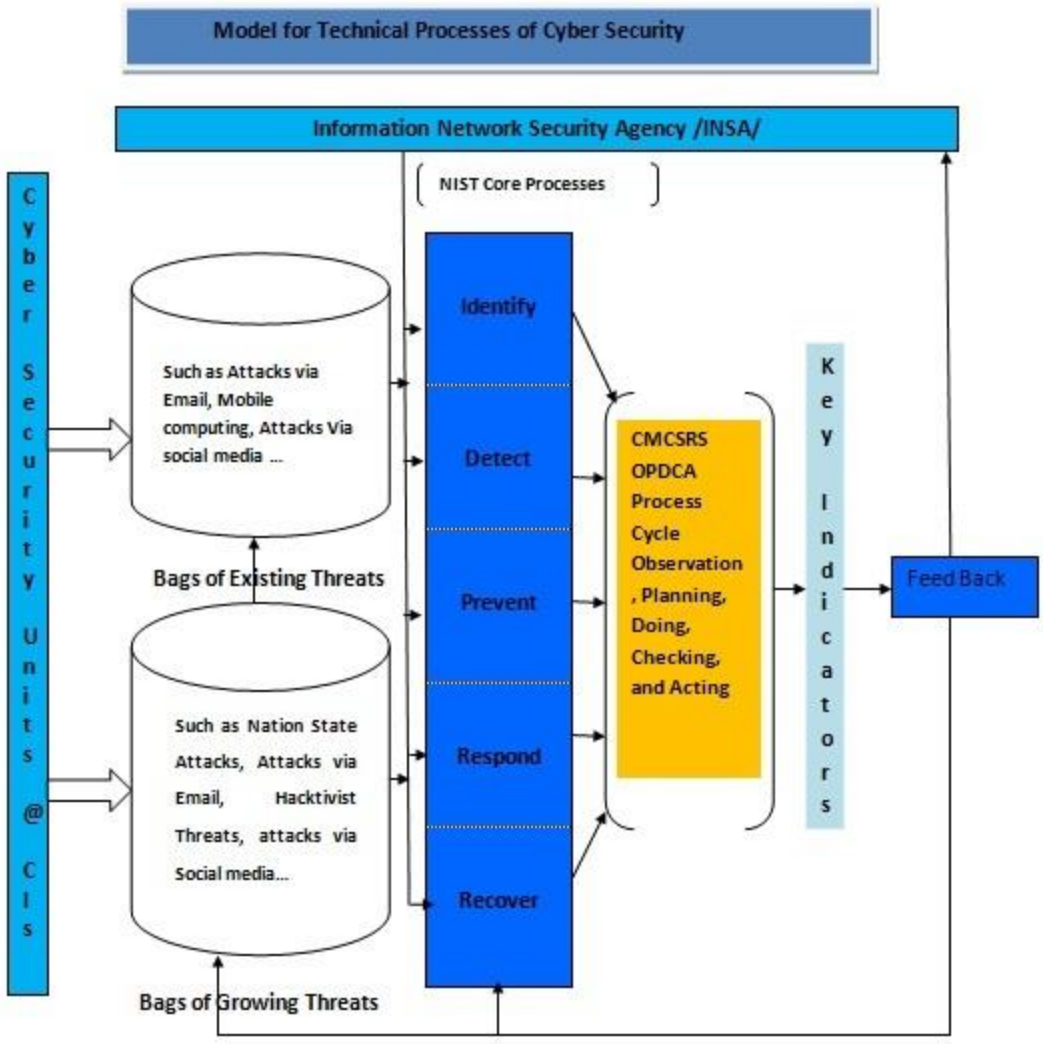


Figure 5.1: Graphical Representation of the Tailored Framework for Technical Processes of Cyber Security

Moreover each NIST core processes performs according to INSA's Critical Mass Cyber Security Requirement Standard process life cycle, OPDCA/observation, Planning, Doing, Checking and Acting/ which is shown in chapter 2 figure 2.5 . Based on the key performance indicators for each NIST core processes, success or failure of the process should be measured. The overall process loops back based on feedback acquired.

3.4 Evaluation of the Proposed Framework

This research used two processes, build and evaluate in tailoring the cyber security framework based on the challenges of cyber security, INSA's Critical Mass Cyber Security Requirement Standard Version 1.0 and NIST framework for improving critical infrastructures cyber security version 1.1.

The tailored framework evaluation is conducted by using questionnaire and interview instruments. With the population of returned questionnaire of 63 with a confidence level of 95% the total of 12 questionnaires are purposefully distributed with return rate of 100%.The questionnaire is tested for reliability with Cronbach's Alpha of 0.842. The proposed framework evaluation survey contains three parts General (which contains Coverage of technical Processes, suitability of the framework and comprehensiveness regarding the content), regarding content of the framework (which contains clarity, correctness and completeness) and regarding utility and applicability of the framework (which includes applicability, fitness with the organization and usefulness to combat cyber threat).

The evaluation survey indicates that 83.3 % the tailored framework covers technical processes adequately. The interview conducted with officer #6 stated that:

> *The five processes are appropriate. It enables us to deal each activity separately".*

This means that the suggested NIST core processes are acceptable and appropriate. Moreover 83.4% of the respondents indicated that the tailored framework is comprehensive regarding its content. However it is only 58.3% of the respondents indicated that it's suitable. Officer #5 stated that:

> *It is a relatively short time since INSA introduced Critical Mass standard. It might not be suitable to modify right now".*

This shows that there is potential for resistance for change. Therefore it's necessary to implement the tailored framework by mandate. Markus and Keil(1994) stated the role of line managers in system implementation as while software suability and line managers behavior in implementing it are very important matters(p.1). This holds to for the tailored framework too.

Considerable number of respondents (73%) indicated that the framework is clear. This result shows that the simplicity and clarity for the framework. Moreover 75% of the respondents indicated that the framework is complete. However its only 50% of the respondents indicated that the framework is applicable. This might be for several reasons. As indicated above there might be a resistance for change or it requires higher management level enforcement.

Finally even if the tailored framework evaluation shows above satisfactory results, some areas need improvement. These are applicability, and suitability.

Chapter six

Conclusion and Recommendations

This chapter presents conclusion and recommendations based on the analysis and findings of the research at critical infrastructures. This portion also lists recommendations for future research.

6.1 Conclusion

This research is the study of cyber security practices and challenges at critical infrastructures in Ethiopia towards tailoring cyber security framework. According to Federal Democratic Republic of Ethiopia council of Ministers Regulation No. 130/2006 define critical infrastructures as any infrastructure vulnerable to information communication network security threats having considerable impact to social, economic or political interests of the country. Similarly US department of home land security and presidential policy directive PPD – 21 identified 16 critical infrastructure sectors. Based on this research identified three critical infrastructures to study the practices and challenges of cyber security. These are Ethiopian Electric Power, Ethiopian Electric Utility and Ethio Telecom.

This research targets to answer three research questions related to challenges, practices and cyber security framework. In order to fully address these research questions , international Telecommunication Union's/ITU/ global cyber security Agendas are used as study pillars namely the legal , technical , cooperation, capability building and organization. The technical pillar is merged with NIST frame work Core process namely identify , detect, prevent, respond and recover in order to identify the practices, and the challenges of cyber security at critical infrastructures.

This research used both quantitative survey and purposefully selected interviews are conducted to collect data. The quantitative survey is conducted by using questionnaire which was adapted and modified from International Telecommunication Union's/ITU/ Global cyber security Index 2017 questionnaire and MIT Technology Review Customs from their research in 2016 cyber security challenges , risks, trends , and impact.

The questionnaire used eight items from MIT Technology review to identify the challenges of cyber security at selected three critical infrastructures namely Lack of in-house Expertise, inadequate enabling technology , insufficient funding , evasion of existing security controls , difficulty in locating right security alert , poor leadership and loss of sensitive or confidential data from mobile and non mobile resources.

The questionnaire used six items to identify the growth trend of cyber threats. Similarly six to seven items are used in the questionnaire to identify the level of preparedness for cyber security threats and breaches in respect to detect, prevent and respond. Finally the questionnaire used three items namely to recruit, develop and retain human resources. All the items used Lickert scale from 1 through 5 is used to collect data from the respondents. The questionnaire also includes items to collect the data concerning the understanding of management team or executives at the highest level of cyber security threat or exposure. The questionnaire is tested for reliability with the overall score of Cronbach's alpha 0.892.

Based on the analysis and the findings, the following five conclusions are drawn from the study:

- The selected critical infrastructures are inadequately prepared to recruit, develop and retain talent within the critical infrastructures. Similarly on job training national or international security related certifications are neglected at critical infrastructures even if cyber security is vital for these organizations.
- The top four challenges at selected critical infrastructures are lack of in-house expertise, inadequate enabling technology, difficulty in locating the right security alert and evasion of preventive security controls. Similarly critical infrastructures faced challenges related to insufficient funding, poor leadership and loss of sensitive or confidential data from non mobile resources.
- The study identified that attack via Email is on growing trend of cyber security threats. In addition attacks via mobile computing, social media, new application development and implementation, and employee's devices or apps /BYOD or BYOA/ are on a growing trend of cyber security threats.

- The study indicated that the selected critical infrastructures are inadequately prepared to detect, prevent and respond to Hacktivist threats, attacks via email, attacks via social media, criminal threats, nation state attacks and insider threats.
- The executive branches at selected critical infrastructures are inadequately prepared to prevent and respond to cyber security threats and breaches.

6.2 Recommendations

The findings and the conclusions drawn in this research pin points the challenges, the trends of growth, and level of preparedness of cyber security and cyber threats or exposure at critical infrastructures for cyber security units' /CSUs/ and for INSA at large. Based on the findings and the conclusion drawn, this research recommends:

- The research recommends the tailored model or framework for technical processes of cyber security at critical infrastructures in Ethiopia. This model enables the stake holders to specifically tackle existing cyber security threats and potential cyber security threats separately by using five core process of NIST framework.
- The executive branches or the highest level of management should acquire appropriate training/skill and knowledge/ in order to enhance their capability in preventing and responding to cyber security threats or exposure.
- Critical infrastructures should develop a capability building framework which makes them capable to recruit, develop and retain security staff.
- The critical infrastructures should formulate or update their policies of using cooperate IT infrastructure for E-mail, social networking, and Employees Mobile devices /BYOD or BYOA/.
- The critical infrastructures and INSA should identify the existing and growing threats and formulate a strategy to combat these threats periodically.

6.3 Recommendations for Future Research

The study recommends the following areas for future research:

- Implementation framework for technical processes of cyber security at critical infrastructures.

Further study should be done on implementation framework for technical process for cyber security at critical infrastructures based on NIST framework of updated version.

- Periodic and comparative Study should be conducted on INSA's Critical Mass Cyber security requirement Standard and its implementation at critical infrastructure.
- The challenges and level of preparedness for cyber security threats and exposure should be examined by using NIST framework and other cyber security frameworks periodically.

References

Abeselom Negussie(2015). Practices, Challenges and Prospects of Information Security in Ethiopian Banking Industry, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

Alen R. Hevner, Salvatore T. March, and JinsooPark(2004). Design Science in Information Systems Research. MIS Quarterly, Vol 28 No. 1, pp.75-105

Aychiluhim Desisa&Tebebe Besha (2014).Internet Banking Security Framework: The case of Ethiopian Banking Industry,HiLCoE Journal of Computer Science and Technology, Vol. 2, No. 2.

An AIAA decision Paper(2017). The World's forum for Aerospace leadership 2017, The connectivity Challenge: Protecting Critical Assets in Networked World, A framework For Aviation Cyber Security.

BBC News (2017).'Massive Equifax data breach' 08-09-2017. Webpage.>http://www.bbc.co.uk/news/bussiness-41192163<. [Accessed 20.09.2017].

Bahabtu Amare (2015). Assessment of Insider Threat in Ethiopian Banking Industry, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

Carrie William (2007). Research Methods, Journal of Business and Economics Research, Volume 5, Number 3.

CNN News (2017). 'North Korea Hackers Stole US-South Korea War Plans' 11-10-2017. Webpage.>http://edition.cnn.com/2017/1010/politics/north-korea-hackers-us-south-korea-war-plan/index.htm<. [Accessed 02.11.2017].

Craig A. Horne , Atif Ahmed & Sean B. Maynard (2016). A Theory on Information Security, Australasian Conference on Information Systems.

Cristin Goodwin & J. Paul Nicholas (2015). A framework for Cyber Security Information Sharing and Risk Reduction, Microsoft Cooperation.

Chwan-Hwa(John) Wu & J.David Irwin(2013). Introduction to Computer Networks and Cyber Security, CRC Press Taylor and Francis Group, India.

Chee-WooiTen ,GovindarasuManimaran& Chen-Ching Liu(2010). Cyber security For Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man and Cybernetics –Part A: System and Humans, Vol. 40, No. 40. Pp.853-865.

Daniel Gebrehawariat (2017). Assessment of the Effectiveness of Card Banking Security in Ethiopian Financial Sector, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

Dictionary of Computing & Communications (2003). Sixth Edition,McGraw-Hill,Newyork.

E Kritzinger& SH Von Solms(2012). A Framework for Cyber security in Africa, Journal of Information assurance and Cyber Security, Vol.2012 (2012).

Elo S. &Kyngash (2008). The Qualitative Content Analysis Process, Journal of Advanced Nursing ,62(1),107-115.

Federal Democratic of Ethiopia (2006). Federal Negarit Gazeta,nformation Network Security Agency Establishment Council of Ministers Regulation No.130/2006,13thYear No. 5 Addis Ababa24th November, 2006, Ethiopia.

Federal Democratic of Ethiopia (2006). The National Information and Communication Technology Policy and Strategy,August 2009, Addis Ababa, Ethiopia.

Federal Democratic of Ethiopia (2012). Federal Negarit Gazeta,Telecom Fraud Offence ProclamationNo. 761/2012,18thYear No. 61 Addis Ababa 4thSeptember, 2012, Ethiopia.

Federal Democratic of Ethiopia Information Network Technology Agency (2016) Critical Mass Cyber Security Requirement Standard Version 1.0

Hamid Salim (2014). Cybersecurity: Systems Thinking and Systems Theory Approaches to Managing Cybersecurity Risk, Massachusetts Institute of Technology, Cambridge.

Halefom Hailu(2015). The State of Cyber Crime Governance in Ethiopia, Addis Ababa, Ethiopia.

International Telecommunication Union, 'Cybersecurity Index /GCI/ 2017' 06/07/2017. webpage>http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx [Accessed 30.10. 2017].

IZ Dlamini, B Taute& J Radebe (2011). Framework for African Policy Towards Creating Cyber Security Awareness,Proceedings of southern African Cyber Security Awareness Workshop(SACSAW), pp.15-31.

Meredyd Williams,Louise Axon, Jason R.C & Sadie Greese(2016). Future Scenarios and Challenges for Security and Privacy, IEEE 2nd International Forum on Research and Technologies for Society and Industry Leverage a Better Tomorrow (RTSI).

Myriam Dunn Cavelty(2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities,Springer.

Mengistu BogaleAyele (2016). Auditing IT and IT Governance in Ethiopia, School of Information Science, Addis Ababa University, and Addis Ababa, Ethiopia.

Nabie Y. Cohteh& Paul J. Schmick(2016). Cyber Security: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks, International Journal of Advanced Computer research , Vol. 6(23).

Rossovw Von Solms& Johan Van Niekerk(2013). From Information Security to Cyber Security,ELSEVIER, Computer & security 38 pp.97-102.

Roderic Broadhurst, Peter Grabosky, Mamoun Alazab and Steve Chon(2014). Organisations and Cyber crime. An analysis of the Nature of Groups engaged in Cyber crime, International Journal of Cyber Criminology, Vol 8 Issue 1 , Janouary 1-June 2014.

Paul Ruggiero & Jon Foote(2011). Cyber Threats to Mobile Phone, US Department of Home Land Security, US-CERT.

Salah Alabady (2009).Design and Implementation of a Network Security Model for Cooperative Network,International Arab Journal of e-Technology, Vol. 1, No. 2

Samar Rahi(2017). Research design and methods: Asystematic Review of research Paradigms, Sampling Issues and Instruments Development International Journal of Economics & management Science, Vol 6 :403.

Satu Elo & Helvi Kyngas (2007). The Qualitative Content analysis Process, journal of Advanced Nursing 62(1), 107-115.

Stephen Herzog (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security, Number 2, Volume 4.

Tariku Adane(2011). Mining Insurance Data Fraud Detection: The case of African Insurance Share Company, School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia.

Tine Hoisgaard Munk (2015). Cybersecuirty in the European Region: Anticipatory Governance and Practices, The University of Warwick.

Tonge, Kasture and Chaudhari(2013). Cybersecuirty Challenges for Society – Literature Review, Journal of Computer Engineering, pp 67-75.

Tilahun Muluneh Arage(2017). A study of Employees' Information Security Policy Violation and Rational Choice Theory: The Case of Ethiopia, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

US Homeland Security (2017). 'Critical Infrastructure Sectors'. Webpage. >https://www.dhs.gov/critical-infrastructure-sectors<. [Accessed 30.10. 2017].

United States General Accounting Office (2004). Technology Assessment Cyber Security for Critical Infrastructure Protection.

White Paper: Enterprise security, Semantics (2009). Anatomy of a Data Breach : Why Breaches happen and What to do about it.

Yoboah-Boateng ,Ezer Osei(2013). Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity and Availability (CIA), (1 ed.), Institut for Elektronisk Systemer, AALBORG University.

APPENDICES

APPENDICES
Appendix A: Letter of Request

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date February 26, 2010
Ref: -SIS/09 /2018

To Whom It May Concern

Student **Tewodros Getaneh** (ID.No. GSE/0384/08) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia towards Tailoring Cyber Security Framework".

I would like to thank you in advance for all the assistance that you would provide to the student.

With Regards,

SCHOOL OF INFORMATION SCIENCE

Martha Yifiru (PhD)
Head, School of Information Science

ethio telecom
የገቢ ደብዳቤ መረከቢያ ቅጽ
ደብዳቤው ገቢ የሆነበት ቀን 29 MAR 2018
የኢትዮ ቴሌኮም ስልክ ቁጥር 0115515700
ደብዳቤውን የተቀበሉት ሠራተኛ ስም Sela
ፊርማ

✉: 1176 ☎: +251-(11)-122-91-91 ☎:2

Appendix B: Questionnaire Survey

Addis Ababa University
School of Graduate Studies College of Natural Science
Department of Information Science

Dear Sir or Madam:

In partial fulfillment of the requirements for the Degree of Master of Science in Information Science, I am undertaking a research on **"Cyber security Practices and Challenges at Critical Infrastructure in Ethiopia: Towards Tailoring Cyber Security Framework"**, at Addis Ababa University. This Study is a case study of three organizations, ***Ethiopian Electric Power, Ethiopian Electric Utility***, and Ethio ***Telecom***. I have accordingly prepared this survey questionnaire. The objective of the survey is to investigate the practices and Challenges of Cyber security Based on five pillars: Legal, Technical, organization, Capability building and Cooperation.

This research is believed to produce results that can improve the protection of Cyber security in respective organization. Your honest responses to each question and statement are extremely valuable to the outcome of this research. The questionnaire survey will take approximately 25 minutes to complete and the results of the survey will be used for the purpose of academic research only. Hence, all responses will be kept in strict confidentiality and hence would not affect any one in any case.

Your dedication is most valued and appreciated and I would like to take this opportunity to thank you in advance for your kind participation, genuine and on time response to the questionnaire.

Thank you again!

Tewodros Getaneh

General Instructions
Please Tick (✓) on the appropriate responses to the questions using the following Likert

Scale:

1 = Strongly Disagree	1= Inadequately Prepared	1 = Inadequately Prepared
2 = Disagree	2 = Somewhat inadequately Prepared	2 = Somewhat inadequately Prepared
3 = Undecided	3 = Somewhat Prepared	3 = Somewhat Prepared
4 = Agree	4 = Well Prepared	4 = Well Prepared
5 = Strongly Agree	5 = Extremely Well Prepared	5 = Extremely Well Prepared

		Strongly Disagree (1)	Disagree (2)	Undecided (3)	Agree (4)	Strongly Agree (5)
I. Cyber Security Challenges						
a. How do your rate your organization top information security challenges?						
1.	Lack of in-house Expertise	1	2	3	4	5
2.	Inadequate Enabling Technology	1	2	3	4	5
3.	Insufficient Funding	1	2	3	4	5
4.	Evasion of Existing Preventive Security Controls	1	2	3	4	5
5.	Difficulty in Locating Right security alert	1	2	3	4	5
6.	Loss of Sensitive or confidential Data.(non mobile Resources)	1	2	3	4	5
7.	Loss of Mobile Devices Containing Sensitive/Confidential Data	1	2	3	4	5
8.	Poor Leadership	1	2	3	4	5
b. Where do you see the most growth in security threats?						
1.	Mobile Computing	1	2	3	4	5
2.	Employee mobile-Device or Application Use/BYOD or BYOA/	1	2	3	4	5
3.	Attack Via E-mail	1	2	3	4	5
4.	New App Implementation/ App Development Process	1	2	3	4	5
5.	Attacks Via Social Media	1	2	3	4	5

6.	Nation on Nation Breach	1	2	3	4	5
II. Detect Sub Pillar						
a. How prepared is your organization to **detect** each of the following kinds of security threats?		**Inadequately Prepared (1)**	**Somewhat inadequately Prepared (2)**	**Somewhat Prepared (3)**	**Well Prepared (4)**	**Extremely Well Prepared (5)**
1.	Insider attacks	1	2	3	4	5
2.	Criminal Threats	1	2	3	4	5
3.	Attack Via E-mail	1	2	3	4	5
4.	Nation State Attack	1	2	3	4	5
5.	Hacktivist Threat	1	2	3	4	5
6.	Attacks Via Social Media	1	2	3	4	5
III. Protect Sub Pillar						
b. How prepared is your organization to **prevent** each of the following kinds of security threats?						
1.	Insider attacks	1	2	3	4	5
2.	Criminal Threats	1	2	3	4	5
3.	Attack Via E-mail	1	2	3	4	5
4.	Nation State Attack	1	2	3	4	5
5.	Hacktivist Threat	1	2	3	4	5
6.	Attacks Via Social Media	1	2	3	4	5
7.	Executive Branch Response	1	2	3	4	5
c. How do you rate your organization's level of security in each of the following areas?		**Inadequately secure (1)**	**Somewhat inadequately secure (2)**	**Somewhat secure (3)**	**Secure (4)**	**Extremely Secure (5)**
1.	Mobile Computing	1	2	3	4	5
2.	Employee mobile-Device or Application Use/BYOD or BYOA/	1	2	3	4	5
3.	Attack Via E-mail	1	2	3	4	5
4.	New App Implementation/ App Development Process	1	2	3	4	5
5.	Attacks Via Social Media	1	2	3	4	5
6.	Nation on Nation Breach	1	2	3	4	5
IV. Respond Sub Pillar						
a.How Prepared is your organization to **respond** each of the following kinds		**Inadequately Prepared (1)**	**Somewhat inadequately Prepared (2)**	**Somewhat Prepared (3)**	**Well Prepared (4)**	**Extremely Well Prepared (5)**

of security Threats?						
1.	Insider attacks	1	2	3	4	5
2.	Criminal Threats	1	2	3	4	5
3.	Attacks Via Social Media	1	2	3	4	5
4.	Attack Via E-mail	1	2	3	4	5
5.	Nation State Attack	1	2	3	4	5
6.	Hacktivist Threat	1	2	3	4	5
7.	Executive Branch Response	1	2	3	4	5
V. Human Resource Sub Pillar						
a. To what extent is your organization able to recruit, develop, and retain security talent?						
1.	Recruit Talent	1	2	3	4	5
2.	Develop Talent	1	2	3	4	5
3.	Retain Talent	1	2	3	4	5

b.For each of these security and risk-related functions, does your organization have human resource and skills needed to adequately address them?		**Yes**	**No**	**I don't Know**
1.	Risk Management	☐	☐	☐
2.	Auditing	☐	☐	☐
3.	Monitoring	☐	☐	☐
4.	Incident Response	☐	☐	☐
5.	Implementation	☐	☐	☐
c. Do you believe the management team or executives at the highest level of your organization truly understand the time and resources needed to mitigate risk and minimize cyber threat exposure?		**Yes**	**No**	**I don't know**
		☐	☐	☐

c. For which of the following security and risk related functions does your organization currently use third-party service providers? **(You can select all that apply)**

a. Auditing
b. Implementations
c. Monitoring
d. Risk management
e. Incident response f. Other _____

Demographic Information

1. Please indicate your educational status
   a. PHD b.MSC c. BSC d. TVET Level
2. What kind of Cyber security / Security Certification do you have?

a. International b. National c. I don't have certification in cyber security /Security

3. Please indicate your organization.

a. Ethiopian Electric Power b. Ethiopian Electric Utility

b. Ethio Telecom d. Ethiopian Air Lines

4. Please indicate your seniority/ Service year in organization

_____ < 2 years _____ 2-5 years _____ 6-10 years

_____ 11-15 year's _____ > 15 year

Appendix C: Interview Outline

Interview outline

I. Challenges of Cyber security at Critical Infrastructures

1. What are the top cyber security challenges in your organization?
2. Where do you see the growth in cyber security threat?
3. How prepared is your organization to detect Cybersecurity breach?
4. How prepared are you to respond to cyber security threat?
5. What is the focus area of cyber security training?

II. Processes and Practices of Cyber security at Critical Infrastructure

1. What are the processes and practices to identify cyber security threat?
2. What are the processes and practices to detect cyber security breach?
3. What are the processes and practices to prevent cyber security threat?
4. How prepared is you organization to prevent cyber security threat?
5. What are the processes and practices to respond to cyber security threat?

III. Inputs for the Framework

1. Do you have any recovery strategy in case of cyber security breach?
2. Do you provide cyber security awareness training for employees?
3. What is the level of compliance for security controls by employees?
4. Do you have cyber security strategy?
5. How frequently does you organization interact with INSA in aspect of Cyber security?
6. Does your organization participate in an international cyber security event, and training?
7. Do you work with local private institutions in aspect of security?
8. Do you think the cyber security budget and human resource are adequate to identify, prevent, detect, respond and recover from cyber security threat and breach?

Appendix D: Proposed Framework Evaluation Survey

Addis Ababa University

College of Natural Science

Department of Information Science

Dear Sir or Madam:

In partial fulfillment of the requirements for the Degree of Master of Science in Information Science, I am undertaking a research on **"Cyber security Practices and Challenges at Critical Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework"** at Addis Ababa University. Based on the findings of the survey to identify the challenges and the practices of cyber security at critical infrastructures namely Ethiopian Electric Power, Ethiopian Electric Utility and Ethio Telecom , I proposed a tailored cyber security framework based on INSA's Critical mass Cyber Security Requirement Standard Version 1.0 and NIST framework to improve critical infrastructure cyber security. The objective of the survey is to evaluate the proposed framework with respect to its comprehensiveness, clarity, completeness, correctness, and applicability.

This research is believed to produce results that can improve in securing cyber space at critical infrastructures.

Thank you for your dedication to provide your genuine feedback regarding the proposed framework.

Thank you again!

Tewodros Getaneh

General

1. The proposed framework is comprehensive in terms of coverage of capability Building and Technical Processes.

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

2. The organization and presentation of the framework is suitable.

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

3. The objective of the four dimensions (Management, People, Process and Technology) is Comprehendible.

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

4. The objective of the framework is comprehensible Regarding the content of the framework

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

Regarding the content of the Framework

5. The content of the proposed framework is clear.

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

6. The content of the proposed framework is correct.

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

7. The content of the proposed framework is complete.

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

Regarding utility and applicability of the framework

8. The proposed framework is applicable.

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

9. The implementation of the proposed framework fits with the organization

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

10. The applicability of the proposed framework can improve Cyber security at critical infrastructures.

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