

**ADMAS UNIVERSITY**  
**POSTGRADUATE PROGRAM**  
**MBA PROGRAM**



**FACTORS AFFECTING GROWTH OF CYBERSECURITY BUSINESS IN  
ETHIOPIA**

---

**In Partial Fulfillment of the Requirements for the Degree of  
Master of Business Administration**

**By: HENOCK ADUGNA**

**Advisor: HAILEMARIAM G. (Ph.D)**

**JUNE 2020**

## Declaration

I, Henock the undersigned, declare that this thesis entitled factors affecting cyber business growth in Ethiopia is the original work I have undertaken the research work independently with the guidance, and support of the research advisor. This study has not been submitted for any degree or diploma program in this or any other institution, and that all sources of materials used for the thesis have been duly acknowledged.

Declared by

Name

Signature

Department

Date

IJSER

## Certificate of Approval of Thesis

School of Postgraduate Studies

Admas University

This is to certify that the thesis prepared by Henock Adugna Sade entitled factors affecting cyber business growth in Ethiopia, and submitted in partial fulfillment of the requirements for the degree of masters of business administration MBA as Business administration Complies with the regulations of the University, and meets the accepted standards concerning the originality, and quality.

Name of Candidate Henock Adugna Sade                      Signature                      Date

Name of Candidate Hailemariam G. (PhD)                      Signature                      Date

Signature of Board of Examiner's

External Examiner:                      Signature                      Date

Internal Examiner:                      Signature                      Date

Dean, SGS:                      Signature                      Date



## Table of Content

Declaration.....	1
Certificate of Approval of Thesis.....	2
Table of Content .....	3
List of figures.....	5
List of Abbreviations, Terminology, and Definition of terms.....	6
Abstract.....	9
CHAPTER ONE: INTRODUCTION.....	10
1.1. Background of the study.....	10
1.2. Statement of the problem .....	11
1.3. Objective Of the study.....	12
1.3.1. General objective .....	12
1.3.2. Specific objective .....	12
1.4. Hypothesis of the study.....	12
1.5. Significant of the Study.....	13
1.6. Scope of the study .....	13
1.7. Limitation of the study .....	14
1.8. Organization of the paper.....	14
CHAPTER TWO: RELATED LITERATURE REVIEW.....	15
2.1 Definition of Constructs.....	15
2.2 Theoretical Literature .....	15
2.2.1What is Cybersecurity?.....	15
2.2.2What Cybersecurity firms do? .....	16
2.3 Theoretical Literature .....	16
2.3.1Cybersecurity Business Globally? .....	16
2.3.2Global cybersecurity market size.....	16
2.3.3Cybersecurity business North America.....	17
2.3.4Cybersecurity business Europe.....	18
2.3.5Cybersecurity business Asia.....	19
2.3.6Cybersecurity business Middle East, and Africa .....	19
2.3.7Cybersecurity business Ethiopia .....	20
2.4 Empirical Literature .....	21

2.4.1 Drivers to the Growth in Cybersecurity business .....	21
2.5 Conceptual Framework .....	26
2.5.1 Description of variables .....	27
2.5.1.1 Dependent Variable .....	27
2.5.1.2 Independent Variables .....	27
CHAPTER THREE: RESEARCH METHODOLOGY .....	30
3.1 Research Setting .....	30
3.2 Study Area .....	30
3.2. Target Population .....	30
3.3. Sampling size .....	31
3.4. Sampling technique .....	31
3.5. Source of Data .....	32
3.6. Data Collection Method .....	32
3.7. Reliability Test .....	33
3.8. Data Processing .....	33
3.9. Data Analysis .....	34
3.10. Data Presentation .....	34
3.11. Ethical Consideration .....	35
CHAPTER FOUR: DATA ANALYSIS, and INTERPRETATION .....	36
4.1 Introduction .....	36
4.2 Profiles of Respondents .....	37
4.2.1 Gender of the Respondent .....	37
4.2.2 Age of the Respondent .....	38
4.2.3 Level of Education of the Respondent .....	39
4.2.4 Work experience of the Respondents .....	40
4.2.5 Occupation of the Respondents .....	41
4.3 Results, and Interpretations .....	41
4.3.1 Analysis of Cybersecurity awareness .....	41
4.3.2 Analysis of Cyber Legislation .....	42
4.3.3 Analysis of Cyber Skilled Manpower .....	45
4.3.4 Analysis of Cyber Firms .....	45
4.3.5 Analysis of Government business policy .....	46
4.3.6 Analysis of Cyber Incident .....	47

4.3.7 Analysis based on mean, and standard deviation .....	48
4.4 Results of Correlation Analysis .....	50
4.5 Results of Regression Analysis .....	52
4.6 Hypotheses Test .....	58
Chapter Five: Summary, Conclusion, and Recommendation .....	61
5.1 Summary, and major findings.....	61
5.2 Conclusion .....	63
5.3 Recommendation .....	63
References .....	65
Appendix .....	67

### List of figures

Figure 1: Conceptual framework for factors affecting cyber business growth. ....	26
Figure 2: Gender of Respondents.....	38
Figure 3: Age of Respondents.....	39
Figure 4: Educational Status of Respondents .....	40
Figure 5: Work Experience of Respondents .....	40
Figure 6: Occupation of Respondents.....	41
Figure 7: Scatterplot of Frequency Distribution .....	56
Figure 8 Histogram of Frequency Distribution.....	56

## List of Tables

Table i-1 List of Terminology, and Definition .....	7
Table 3.1 Sample Size Determination Table .....	31
Table 4.1 Profile of the respondent.....	37
Table 4.2 Analysis of Cyber awareness .....	42
Table 4.3 Analysis of Cyber Legislation .....	42
Table 4.4 Analysis of Cyber Solution Demand .....	43
Table 4.5 Analysis of Cyber Skilled manpower .....	45
Table 4.6: Analysis of Cybersecurity Firms .....	46
Table 4.7: Analysis of Government Business Policy.....	47
Table 4.8: Analysis of Cyber Incident .....	50
Table 4.9: Results of Correlation Matrix .....	50
Table 4.10: Measure of Quality of Prediction .....	50
Table 4.11 ANOVA .....	53
Table 4.12: Regression Result for Cyber Business growth .....	54
Table 4.13: Residuals Statistics of Cyber Business Growth.....	55
Table 4.14 Hypothesis Testing/Accepted or Rejected.....	58
Table 6.1 Questionnaires .....	70

## List of Abbreviations, Terminology, and Definition of terms

Table i-1 List of Terminology, and Definition

Terminology	Definition of terms
Cyber actors	Employees of organizations, hackers, cyber experts, ICT Directors, CEO of organizations, and those who participate in the cyber environment.
Cyber:	Anything related to networks, computer, internet, mobile, and electromagnetic devices in which capable of processing, and analyzing information, and data
Cyber legislation	That legislation is prepared to control the cyber environment of firms like ICT policy, email policy, password policy, and other governance legislations of firms.
Cyber awareness	The level of understanding of the cyber environment, and terminologies, tools, techniques, and related issues.
Cyber business	Any business related to security, digitalization, and infrastructure.
GBS	Government Business Policy
CI	Cyber Incident (might be cyber-crime, theft, and cyber-attack.
CSD	Cyber Solution Demand
CSA	Cybersecurity Awareness
CL	Cyber Legislation
SM	Skilled Manpower
INSA:	Information network security agency
Cyber Incident	Any occurrence of the cyber incident it may be an attack or fraud or theft, and including cybercrime
0Cyber Business	Anything related to software, Hardware, Mobiles, Telecom, infrastructure, and electromagnetic business activity
Cyber environment	Software, network, internet, computer, mobile devices, and anything related to information management environment.



## **Acknowledgment**

First I would like to thank God for supporting me from start to end in which I was under working under pressure, and also on this current Covid-19 issues which are difficult, and challenging time,

Secondly, I would like to thank Hailemariam G. (Ph.D.) for his commitments, and passion to support, and guidance this work besides those peoples who helped me with ideas Dr. Mehari (Ph.D.), and Makonnen.

3<sup>rd</sup> for my beloved wife for her patience, and holding the burden of the house on this challenging time.

IJSER

## Abstract

*The purpose of this study is to investigate and explore the factors that affect cyber business growth in Ethiopia. To achieve the objective, the study adopted an explanatory research design. From a population of 993, the study would be taken a sample size of 232 respondents and is chosen on a convenient basis. 82.75% (191 respondents) valid response rate is yielded. The primary data would be used for the study, and a structured questionnaire with a 5-point Likert scale has been used to collect the data by conducting a survey. A pilot test would be conducted to test for validity and reliability. Because of COVID-19, it is hard to distribute the questionnaires physically. The study would be used as an online questionnaire using a google form method to collect the data. The data has been analyzed by using Statistical Package for Social Sciences software (version: 25) for descriptive statistics which included frequency distribution tables, mean, standard deviation, one-sample t-test, correlation, and regression. The data has been presented using tables, and charts for ease of understanding the results. The result of the study showed that increasing cyber firms, skilled manpower, Government business policy, and legislations, and solution demand significantly, and positively influenced cyber business growth. The recommendation made was that the government must take a necessary measure to improve business policy especially for the cyber sector, and also government must focus on encouragement to look at the dimensions used (increasing solution demand, improving skilled manpower in the cyber sector, and encouraging startup firms in the cyber sector).*

**Keywords:** Cyber, Cyber Business, Cyber Business Growth, Business Growth, Government Business Policy, and Cyber Awareness.

## CHAPTER ONE

### INTRODUCTION

#### 1.1. Background of the study

Now a day's cyber-crime and its security become a day to day concern in everyone's life. the world so far lost \$53 billion per year by cyber-attack. Cybercrime damages are anticipated to cost businesses, and organizations \$6 trillion annually by 2021, according to the 2019 ACR from Cybersecurity Ventures. This number, which is up from the company's 2015 estimate of \$3 trillion in cybercrime damages annually, "represents the greatest transfer of economic wealth in history, risks the incentives for innovation, and investment, and will be more profitable than the global trade of all major illegal drugs combined (Herjavec Group, 2020).

Also, countries are increasing their budget which will be spent on cybersecurity, even the USA only budgeted for cybersecurity \$17.4 Billion for 2020 which is almost equivalent to the 2020 Ethiopian yearly budget (Whitehouse, 2020).

Cybersecurity businesses are providing a security solution for businesses and government organizations. By definition, A successful cybersecurity approach has multiple layers of protection spread across the computers, servers, mobile devices, electronic systems, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber-attacks. (Cisco, 2020) Now a day's cyber-attack comes in different shape and mechanisms. It is going to be beyond the computer, and internet infrastructure. As we are in the information age, we need to be aware of every challenge that came with digitalization, and security.

The cybersecurity business is continuously increasing its growth globally. The market share of the global cybersecurity market value stood at USD 112.01 billion in 2019 and is projected to reach USD 281.74 billion by 2027 (Fortunebusinessinsights, 2020).

The adoption of cybersecurity solutions is expected to grow with the increasing penetration of the internet among developing and developed countries. Also, the expanding wireless network for

mobile devices has increased data vulnerability making cybersecurity an integral part of every single organization across the world (Dublin, 2019).

Central government working on protecting key government organizations, and infrastructures by establishing a national cyber defense organization which is INSA. but still, the issue is beyond government control. Mainly it needs private sector engagement for the successful implementation of cyber power and protecting the country against attack (INSA, 2014).

For this thesis, the main tool which is used to perform the assessment, and analysis is a secondary source of data, and questioners collected from the management of different cyber business firms.

## **1.2. Statement of the Problem**

Ethiopian business environment is challenging for startup and mature Cybersecurity firms to sustain, and grow. many startups and mature cyber firms are challenged by different challenges like lack cyber awareness of the society, and sustaining on the business, the national cyber policy, and finding cybersecurity Experts. Most of them are early to exit their firms. Besides, the cyber environment seems the means of corruption.

The other challenge is the country didn't get the expected benefit from the sector, and also the increasing number of cyber-attacks on financial, and key government, and public organizations are negatively impacted investors to as not to invest in their full confidence. From the social, and political perspective, society have might get attack by social media, if it has been a victim of cyber-attack, it has a huge impact on social, and political, psychological as well economic crises.

Identifying those factors that affect the business firm will help the government to take the necessary measure to improve and encourage the business environment. Otherwise, if the cyber business firms didn't get special attention, and grow, the government cannot control the effect that came with cyber-attack so the government should help to solve those factors that affect the private, and public cyber business growth.

Finally, the demand for cyber-solutions is high, and continuous in the global market but the cybersecurity status in Ethiopia is still ranked around last in the least. For Example, From the perspective of the National Cybersecurity Index stated Ethiopia ranked 105th in the Global

cybersecurity Index and 84th in National Cybersecurity Index in the world. This research answers or illustrates those factors that affect cybersecurity business growth (EGA, 2020).

### **1.3. Objective Of the study**

#### **1.3.1. General objective**

- ☒ To analyze the factors affecting cybersecurity business growth in Ethiopia.

#### **1.3.2. Specific objective**

- ☒ To examine the effect of cybersecurity awareness on cyber business growth.
- ☒ To determine the effect of Cybersecurity Legislation on cyber business growth.
- ☒ To investigate the effect of cyber incidents on cyber business growth.
- ☒ To examine the effect of the Number of cyber firms on cyber business growth.
- ☒ To evaluate the effect of the Demand of cyber solutions on cyber business growth.
- ☒ To examine the effect of Government Business Policy on cybersecurity business growth.
- ☒ To determine the effect of Cybersecurity Skilled Manpower on the cybersecurity business growth.

### **1.4. Hypothesis of the study**

- ☒ H01: Cybersecurity awareness does not have a significant effect on the growth of cyber business growth.
- ☒ Ho2: Cybersecurity Legislations does not have a significant effect on the growth of cyber business growth
- ☒ Ho3: Number of cyber incidents does not have a significant effect on the growth of the cybersecurity business.
- ☒ Ho4: Number of cyber firms does not have a significant effect on the growth of the cybersecurity business.
- ☒ Ho5: The demand for cybersecurity solutions does not have a significant effect on the growth of the cybersecurity business.

- ✎ Ho6: Government Business Policy does not have a significant effect on the growth of the cybersecurity business.
- ✎ Ho7: Cybersecurity Skilled Manpower does not have a significant effect on the growth of cybersecurity business.

### **1.5. Significant of the Study**

this thesis has a significant contribution to different stakeholders. Major stakeholders of this thesis are Government, Students, Investors, business owners, policymakers, and others that are not listed on this document.

This thesis has a major significance in the following way

- ✎ It is used for Government as input for preparing National Cyber-Security Policy, and Strategic Direction.
- ✎ It provides options for investors who would like to invest in the cybersecurity business in Ethiopia.
- ✎ It is used for students who are working on cybersecurity, and business growth as an educational reference, investors, and researchers what the Cybersecurity situation Looks like in Ethiopia.
- ✎ It is Used for Security Agencies for the preparation of their cybersecurity strategic roadmaps.
- ✎ It is used for importers as an input for their investment options.
- ✎ It is used for software firms as an input for their investment options.
- ✎ It is used for ICT infrastructure firms as an input for their investment options.
- ✎ It is used for any citizen as an awareness of how security is critical in the coming digitalization world.

### **1.6. Scope of the study**

The scope of the research is analyzing factors affecting cyber business growth in Ethiopia, it is mainly focusing on data collected from organizations ICT Directors, business firm owners, CEOs, Experts in the area, and those who have well information about cyber business in Ethiopia. Besides

information based on existing data collected by government institutions like the ministry of innovation, and ministry of trade for a period of the last 11 years from 2009 to 2020, majorly, and questionnaire survey. The study covers areas related to ICT companies, Telecoms, and electronic device providers.

### **1.7. Limitation of the study**

There are different limitations to conduct this research. Even though, a major limitation of this research proposal is listed as follows

- ✘ Lack of organized data source related to business growth
- ✘ shortcomings of related local researches for reference
- ✘ lack of probability sampling: Because of Corona-COVID-19 situation.
- ✘ Scope of discussions: is large
- ✘ Lack of business demography dataset: a system that registers all business demography data that can help to perform different statistics, and analysis.

### **1.8. Organization of the paper**

In chapter one, the study defines the introduction, background of the study, and its major parts like problem statement, and significance of the study. Chapter two explains about related literature review and conceptual framework of the research. Chapter three illustrates the research methodology., and in chapter four the proposal focuses on findings, and discussion, and chapter five summary, conclusion, and recommendation, and finally Reference.

## CHAPTER TWO

### RELATED LITERATURE REVIEW

#### 2.1 Definition of Constructs

In the following section, two major cornerstones of literature review parts are reviewed. Those parts are theoretical literature review and empirical review. The theoretical review shows the theoretical aspects of cyber, and cyber business in the world, Africa, and Ethiopia. Whereas in the Empirical part major predictors of cyber business are identified, and the study of others is stated.

#### 2.2 Theoretical Literature

##### 2.2.1 What is Cybersecurity?

There is no standard, universally accepted definition of cybersecurity<sup>1</sup>. Broadly, it is all the safeguards, and measures adopted to defend information systems, and their users against unauthorized access, attack, and damage to ensure the confidentiality, integrity, and availability of data. Cybersecurity involves preventing, detecting, responding to, and recovering from cyber incidents. Incidents may be intended or not, and range, for example, from accidental disclosures of information, to attacks on businesses, and critical infrastructure, to the theft of personal data, and even interference in democratic processes. These can all have wide-ranging harmful effects on individuals, organizations, and communities. As a term used in EU policy circles, cybersecurity is not limited to network and information security. It covers any unlawful activity involving the use of digital technologies in cyberspace. This can, therefore, include cybercrimes like launching computer virus attacks, and non-cash payment fraud, and it can straddle the divide between systems, and content, as with the dissemination of online child sexual abuse material. It can also cover disinformation campaigns to influence the online debate, and suspected electoral interference. Also, Europol sees a convergence between cybercrime, and terrorism (EUROPEAN COURT OF AUDITORS, March 2019).

Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks. It aims to reduce the risk of cyber-



attacks and protect against the unauthorized exploitation of systems, networks, and technologies (itgovernance, 2020).

### **2.2.2 What Cybersecurity firms do?**

Cybersecurity services providers offer a range of solutions related to the protection of computer systems within an organization. Also known as computer security or IT security, cybersecurity is a constantly evolving industry created in response to hacking, viruses, and the various other threats to personal, and professional data. Cybersecurity providers offer expertise along the three stages of business cybersecurity: assessment, protection, and remediation. Businesses are encouraged to supplement external cybersecurity solutions with IT security software, and several services providers offer cybersecurity tools in addition to services. In addition to cybersecurity, there are a variety of IT outsourcing services that can address your company's information technology needs.

## **2.3 Theoretical Literature**

### **2.3.1 Cybersecurity Business Globally?**

A report from Business Insider Intelligence estimated that \$655 billion will be spent on cybersecurity initiatives to protect PCs, mobile devices, and Internet of Things (IoT) devices by 2020, of which \$386 billion will be spent on securing PCs, \$172 billion on securing IoT devices, and \$113 billion will be spent on securing mobile devices. According to Bloomberg, and IDC, the largest areas of growth within cybersecurity are mobile security, the Internet of Things (IoT) security, and specialized threat analysis, and protection (Business Insider , 2020).

### **2.3.2 Global cybersecurity market size**

The cybersecurity market size was valued at \$104.60 billion in 2017 and is projected to reach \$258.99 billion by 2025, growing at a CAGR of 11.9% from 2018 to 2025. Cybersecurity also referred to as Information Technology (IT) security, emphasizes safeguarding computers, programs, networks, and data from unlicensed or spontaneous access. As cyber threats have gained importance, security solutions have progressed as well. Factors such as a rise in malware, and

phishing threats, and growth in adoption of IoT, and BYOD trend among organizations, are driving the cybersecurity industry growth (Author(s) : Makarand Sinnarkar, Mar 2019).

Growing demand for cloud-based cybersecurity solutions is also one of the major factors fueling market growth. However, constant need to conform to cybersecurity industry standards, regulations, and complexities of device security are some of the major factors hampering the market growth. Furthermore, cybersecurity activities are now being prioritized and aligned to strategic business activities to minimize the damage of IT resources, which provides the major opportunity for market growth. Also, an increase in the need for strong authentication techniques is expected to provide lucrative opportunities for the market (Author(s) : Makarand Sinnarkar, Mar 2019).

### **2.3.3 Cybersecurity business North America**

North America Cybersecurity market has rapidly gained traction in the market and is expected to have the fastest growth in the coming years. Organizations are in dire need of solutions that could help them identify, protect, and respond to cyber threats. This requirement has arisen due to the increase of network connection, processing, users, and high dependency on the internet. North America Cybersecurity is one of the alarming concern in many domains such as government, manufacturing, etc. The concept of E-governance has brought major usage of the web thereby increasing threats of cyber-attacks. The government has also increased cyber laws, legal regulatory compliance, and data security. The United Nations (UN), Organization for Security, and Cooperation in Europe (OSCE), and other international organizations have introduced new cybersecurity policies or renewed existing ones. Many organizations are showing their differentiating competencies by introducing specific solutions, and applications to focus on need, and demand on particular security organizations require (Micro Market Monitor, 2017).

The proliferation of cybersecurity business is significant in large enterprises; however, small, and medium organizations are also investing in this market as the benefit associated with it encourages its adoption. However, the popularity of cloud deployment options has given enormous benefits to the organization to focus more on cybersecurity. Mobile security, cloud security is the upcoming focus for cybersecurity market. In the years to come, this trend is anticipated to continue leveraging

cybersecurity solutions, and services providers to offer a more innovative solution to cater to the need for the cloud security required in various sectors. Increasing usage of mobile data for various purposes like social marketing, mobile banking, using various applications has made it more vulnerable to cyber threats (Micro Market Monitor, 2017).

The cybersecurity market is growing due to the evolving trend of Bring Your Device (BYOD). Therefore, the use of personal devices in the workplace continues to rise, so businesses need to think carefully about BYOD, and put in place appropriate policies to tackle these issues. Moreover, this market unfolds various opportunities such as partnerships, and collaboration, mergers, and acquisitions by the developed players for exploring new product lines. Thus, taking into account all these pointers, the cybersecurity market is estimated to further grow substantially in the upcoming years (Micro Market Monitor, 2017).

### **2.3.4 Cybersecurity business Europe**

The Europe Cybersecurity market size is estimated to grow from USD 26.85 billion in 2015 to USD 37.38 billion by 2020, at an estimated CAGR of 6.8% from 2015 to 2020. Cybersecurity products are defined by their capability to provide access management, authentication procedures, detection, and responses to incidents, security updates or patch management, data recovery, mitigation of impacts, and risk, and compliance management. The products are primarily responsible for protecting location where information and communication systems are placed, which consists of servers, storage, network equipment, and virtual machines. The report aims at estimating the market size, and future growth potential of the Europe Cybersecurity market across different segments such as solution, service, vertical, and country. The base year considered for the study is 2014, and the market size is forecasted from 2015 to 2020 (micromarketmonitor, 2015).

The growing number of the mobile workforce, adoption of cloud-based services, and Advanced Persistent Threats (APTs) present a comprehensive opportunity for cyber vendors in the market space. Apart from these, factors such as the need for strict compliance, and data disclosure mandates, risk over maintenance of sensitive data, increased Internet penetration, and increasing spending patterns on security forums are boosting up the demand for cybersecurity solutions. It is

expected that the cyber market in European countries will show enormous growth with credence in the coming years (micromarketmonitor, 2015).

### **2.3.5 Cybersecurity business Asia**

The Asia-Pacific cybersecurity market is projected to grow from USD 17.19 billion in 2015 to USD 30.39 billion by 2020, at a CAGR of 12.1% from 2015 to 2020. Organizations require solutions, which could help them identify, protect, and respond to cyber threats. Cybersecurity is becoming a major concern among varied industry verticals such as Banking, Financial Services, and Insurance (BFSI), government, IT & telecom, aerospace & defense, retail, and manufacturing. The concept of e-governance has amplified the usage of the web, thereby increasing the occurrence of cyber threats. The government has also increased cyber laws, legal regulatory compliances, and data security (MicroMarketMonitor, 2015).

Cybersecurity products are defined by possessing the capability to provide access management, authentication procedures, detection, and responses to incidents, security updates or patch management, data recovery, mitigation of impacts, and risk & compliance management. The cybersecurity market is experiencing a booming phase because of the need for global cybersecurity capacity establishment built for secure, and resilient cyberspace (MicroMarketMonitor, 2015).

Increasing usage of mobile data for varied applications such as social marketing and mobile banking has made these sectors more vulnerable to cyber threats. Mobile security and cloud security are upcoming applications in the cybersecurity market. In the future, this trend is anticipated to continue leveraging cybersecurity solutions, and services providers (MicroMarketMonitor, 2015).

### **2.3.6 Cybersecurity business the Middle East, and Africa**

The Middle East & Africa Cybersecurity market size is estimated to grow from USD 7.70 billion in 2015 to USD 14.47 billion by 2020, at an estimated CAGR of 13.4% from 2015 to 2020. Cybersecurity products are defined by possessing the capability to provide access management, authentication procedures, detection, and responses to incidents, security updates or patch

management, data recovery, mitigation of impacts, and risk & compliance management (Micro Market Monitor, 2015).

The cybersecurity market is experiencing a booming phase because of the need for global cybersecurity capacity establishment built for secure, and resilient cyberspace. The report aims at estimating the market size, and future growth potential of the Middle East & Africa Cybersecurity market across different segments such as solution, service, vertical, and country. The base year considered for the study is 2014, and the market size is forecasted from 2015 to 2020 (Micro Market Monitor, 2015).

The growing number of mobile workforces, adoption of cloud-based services, and Advanced Persistent Threats (APTs) present a comprehensive opportunity for cyber vendors in the market space. The MEA comprises economies such as Israel, the United Arab Emirates, Egypt, Libya, and so on. These are countries where government regulations are very stringent regarding the Internet, media, publications, surveillance, and monitoring (Micro Market Monitor, 2015).

The main revenue source of the MEA is oil and gas. After the major cyber-attack on oil giant, Saudi Aramco in 2012 leaving tens of thousands of infected PCs, the number of government initiatives as well as investments from countries such as Saudi Arabia, UAE for avoiding future data breaches resulting in significantly increased. This has resulted in the continual expansion of opportunities for cybersecurity vendors across the region. It is expected that the cyber market in Middle East & Africa countries will show enormous growth with credence in the coming years (Micro Market Monitor, 2015).

### **2.3.7 Cybersecurity business Ethiopia**

In 2001, a national task force coordinated by the National Computer, and Information Center of the Ethiopian Science, and Technology Commission initiated Data Disaster Prevention, and Recovery Management (DDPRM) program which mainly sought to address data integrity, and physical security. The objective of this project was to formulate a policy, which facilitates enabling the environment, and paves the way for designing a secure institutional data center. The overall

intention was to protect data stored, processed, and transmitted through the computer system. In addition to this, the project was also supposed to develop guidelines, and procedures that support corporate enterprises to put in place their own organizational data security in house policy. As compared to data security, information security is a broader system which deals with all critical elements, and components of an information system namely: Software, Hardware, Data, People, Procedures, and Networks. Concerning this, the Data Disaster Prevention, and Recovery Management guideline developed by a task force organized by Ethiopian Science, and Technology Commission is a good move towards adopting strategies to determine the level of protection required for applications, systems, facilities in ICT development and recover from any disaster without serious business discontinuity, and major damages, and loss to the system, and data. However, escalation of the specific data security issues to more general information security systems was found to be mandatory (Reba, 2005).

The above paragraph states the effort of the government to secure the cyber environment, but the private sectors are not engaged in the cybersecurity business until 2005. The effort has been started since 2005 in a form of import-export of security devices, sales of antivirus, file recovery, and maintenance, and other security-related software. even though this all private-sector effort goes on still policy cannot support those cyber firms to work aggressively because of this most of the cybersecurity companies are moving from the business.

## 2.4 Empirical Literature

### 2.4.1 Drivers to the Growth in Cybersecurity business

The growth in cybersecurity is primarily driven by the following drivers these drivers are listed bellow

- ✎ The **key drivers** for the cybersecurity market are the **increasing government regulations on data privacy, rising cyber threats, an increasing number of data centers**, which are the most significant revenue generators for the cybersecurity market.
- ✎ The **total number of reported cybersecurity incidents** witnessed a steep increase over the past few years, leading to increased emphasis on data security, and protection. The

**formation of hacking groups that deal with ethical, and large-frame hacking**, causing huge losses, has created a dire need for cybersecurity in the market.

- ✎ Factors hindering the growth of the market are the **lack of awareness** and **availability of pirated cybersecurity solutions**. Several governments across the globe have gradually warmed up to the need for collaborations, and initiatives to counter frequent breaches, and attacks. (MarketWatch, 2020)

The key drivers of this market include Government regulation on data privacy, increasing cyber threats, an increasing number of data centers, which are the biggest revenue generators for Cybersecurity Market. The key restraints to this market are lack of awareness, and availability of pirated security (FMI, 2019).

Another study shows that the industry outlook for cybersecurity is very positive. Due to the increasing number of cyberattacks, the growth expectations for cybersecurity spending going forward are very high. Some of the key growth areas within cybersecurity, such as IoT security, and cloud security, will help drive the growth of this industry. Also, the rising costs of cybercrime and corporations' willingness to spend large amounts on cybersecurity are further justifying these growth expectations for the industry. As a result, continued growth, and increased spending in this space strongly shows that the cybersecurity industry will be a profitable investment for the foreseeable future (solidbridge, 2020).

Markets and Markets stated that the major factors driving the cybersecurity market are an increase in the frequency, and sophistication of cyber-attacks, the emergence of disruptive digital technologies like IoT, stringent data protection regulations for information security, and increase in several supply chain-based attacks exploiting the software supply chain (Markets and Markets, 2018).

### **"Growing Adoption of Cloud-based Services in IT Security to Favor Market Growth"**

One of the key trends that enable the overall growth of the cybersecurity market is the rising adoption of cloud computing. Cybersecurity solutions are based on complex mathematical prediction models, handling large amounts of data. This data monitoring can only be fulfilled by

cloud technology in a secure, and reliable environment at a low cost. Key players such as IBM Corporation, Cisco Systems, and others, are focusing on integrating cloud computing with cybersecurity solutions. These cloud computing services are backed up by ‘Analytics as a Service’ (AaaS) offerings, allowing users to detect, and mitigate uncertain threats quickly (Fortune Business Insights, 2019).

### **"Rising Adoption of E-commerce Platforms, and the advent of Disruptive Technologies to Drive the Market"**

In the present scenario, security related to the IT sector has become the primary concern for the corporate, public, and private division. The growing adoption of e-commerce, and the advancement of disruptive technologies such as artificial intelligence, and blockchain has increased the adoption of cybersecurity solutions in a connected network ecosystem. As per the current market, these factors will enormously boost the cybersecurity market growth in the coming years. (Fortune Business Insights, 2019).

### **"Increasing Investments by Governments in Cybersecurity Solutions to Spur Growth Opportunities"**

Cybersecurity has become an emerging discipline and has driven the focus of many global organizations, and the government to invest in advanced security solutions. In the current period, governments of emerging countries are among the major customers for the cybersecurity solutions due to a huge volume of confidential data, and information. According to a report by the European Cybersecurity Organization, the government in the U.K. invested around USD 2.30 billion for the implementation of various cybersecurity programs in defense, and research. This would help to boost the overall adoption rate for cybersecurity solutions across multiple industries shortly. All these investments, rising focus of the organization, and support from the government of various countries are projected to contribute to the growth of the market in terms of revenue (Fortune Business Insights, 2019).

### **"Limitations Related to High Cost of Innovation, and Budget Constraints for SMEs to Hinder the Market Growth"**



With the growth in the number of cybersecurity threats, and attacking tools, the requirement for advanced cybersecurity solutions to deal with such attacks is growing exponentially. The traditional cybersecurity solutions are not enough accomplished of securing the organizations from advanced threats of cloud, network, endpoint security, among others. Also, huge algorithms are required for cybersecurity solution providers to develop technically advanced solutions. Further, high cost associated with cybersecurity solutions, and services limits the adoption among small, and medium enterprises (Fortune Business Insights, 2019).

### **"Rising Adoption of End-point Security by Enterprises to Boost the Market Growth"**

Based on solutions, the market is divided into network security, cloud application security, end-point security, secure web gateway, internet security, and others. Among these, cybersecurity solutions in end-point security are expected to grow at a gradual CAGR. The cybersecurity solutions in the cloud application security area are expected to grow at the highest CAGR in the forecast years. This growth is owing to the rising investment, and adoption of cloud technology among the various industries including financial institutions, IT & telecom, and others (Fortune Business Insights, 2019).

### **"Rising Investment by Key Players to Boost the Market Growth"**

Based on end-use, the market is segmented into BFSI, IT, and telecommunications, healthcare, government, retail, travel, and transportation, manufacturing, energy, and utilities, and others. Among these industries, BFSI is expected to rise with a gradual CAGR during the forecast period. This growth is attributable to the rising demand for robust security, and digital privacy systems across financial, and banking institutes. Additionally, an increase in the adoption of internet banking, online applications, and cloud are driving the cybersecurity market growth. Cybersecurity solutions are helping banks, insurance, and financial organizations to secure highly confidential data integrated with real-time intelligence against insistent cyber-attacks (Fortune Business Insights, 2019).

### **Cybercrime Legislation Worldwide**

138 countries (of which 95 are developing, and transition economies) had enacted such legislation. However, more than 30 countries had no cybercrime legislation in place (UNCTAD, 2020).

### **E-transactions Legislation Worldwide**

A prerequisite for conducting commercial transactions online is to have e-transaction laws that recognize the legal equivalence between paper-based, and electronic forms of exchange. Such laws have been adopted by 145 countries, of which 104 developing or transition economies. While four out of five countries in Asia, and in Latin America have such laws in place, Eastern, and Middle Africa lag.

### **Data Protection, and Privacy Legislation Worldwide**

107 countries (of which 66 were developing or transition economies) have put in place legislation to secure the protection of data, and privacy. In this area, Asia, and Africa show a similar level of adoption, with less than 40 percent of countries having a law in place.

### **Online Consumer Protection Legislation Worldwide**

Despite the importance of consumer confidence for business-to-consumer e-commerce, many developing, and transition economies still lack laws to protect consumers online. In as many as 67 countries, it was not possible to obtain data, suggesting that online consumer protection is not being fully addressed. Out of the 125 countries for which data exist, 97 (of which 61 are developing or transition economies) have adopted consumer protection legislation that relates to e-commerce. In terms of regional patterns, the incidence of consumer protection laws is particularly low in Africa.

### **Skilled Man Power**

The other factor that affects cyber business is the increasing number of skilled manpower the studies show that there will be 3.5 million unfilled cybersecurity jobs by 2021, and this is the worst situation in Ethiopia. It is not more than two higher education institutes are having cybersecurity program (UNCTAD, 2020).

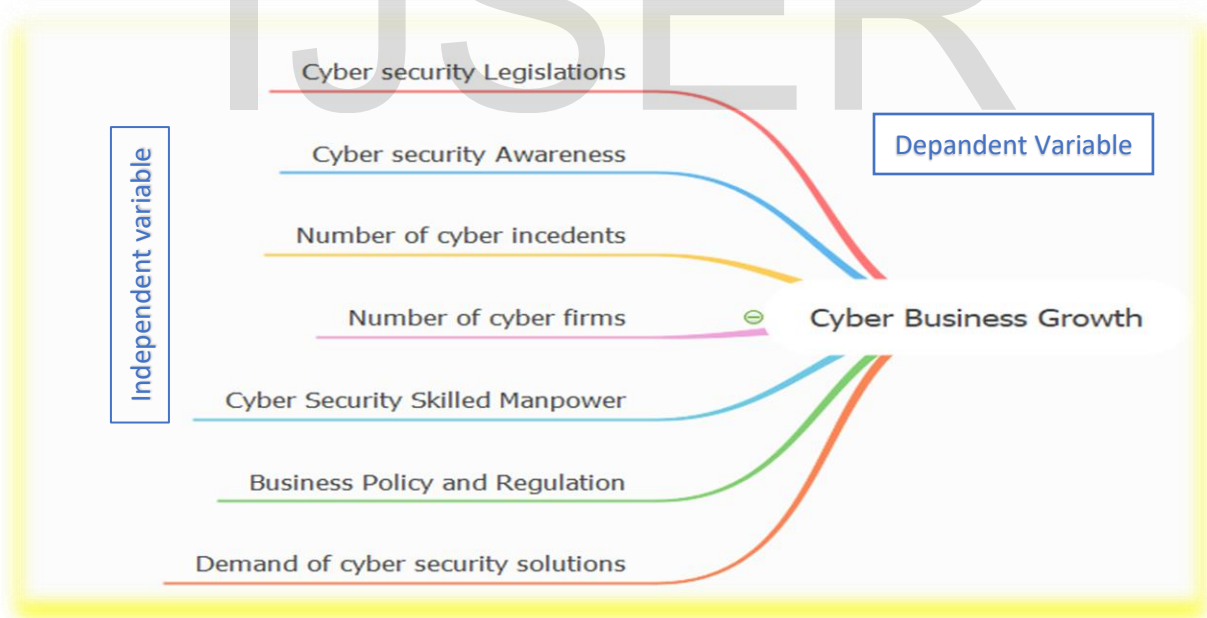
## Ethiopia, and Cyber Legislation

In the case of Ethiopia, Ethiopia Accepts only two of the legislations Electronic Transactions: Legislation, and Cyber Crime: Legislation but the other two legislations like Consumer Protection: No Data, and Privacy, and Data Protection: No Legislation are yet policy is not still developed. This is one of the major factors to grow the cyber business at large (UNCTAD, 2020).

### 2.5 Conceptual Framework

Identification of major dependent and independent variables is key to analyze the factors affecting cyber business firm's growth. So, based on the key variables preparing questioners, and interviews are also important, the next step goes to select the proper candidate cyber actors that helps to do sample data collection., and using the standard tool representing collected data will be the last stage documenting, and submitting the result.

Figure 1: Conceptual framework for factors affecting cyber business growth.



Source: Developed for this study, 2020

## Dependent Variable

- ✎ Cyber Business Growth

## Independent Variables

- ✎ Cybersecurity Legislations
- ✎ Government Business policy, and regulation
- ✎ The demand for cybersecurity solutions
- ✎ Cybersecurity Awareness
- ✎ Number cybersecurity incidents
- ✎ Number of Cyber Firms
- ✎ Cybersecurity Skilled Manpower

### 2.5.1 Description of variables

#### 2.5.1.1 Dependent Variable

- **Cyber Business Growth:**

This variable shows the growth status of the cyber business in Ethiopia, it shows the number of business firms, the number of cyber-attacks, the status of countries protection level from an international perspective like National Cybersecurity Level/Rank, and Global cybersecurity level/Rank.

The growth can be measured based on the following parameters: Cyber Business growth, profitability, employee satisfaction, the sales volume of cyber firms, increase in employments, Increase, and improvement in IT Technologies, and Infrastructure, Cybersecurity Skilled Manpower Development Programs, and societal/cyber stakeholder satisfaction.

#### 2.5.1.2 Independent Variables

- **Cybersecurity Legislation:**

cybersecurity policy is any regulation, proclamation, or procedure which is related to cyber that helps to Guide and control the Global, and National cyber environment. Besides, those policies and procedures that support cyber growth are assessed and identify their implication for the growth of cybersecurity business.

- **Government Business policy, and regulation:**

This is a proclamation, procedure, or any regulation or framework that must be followed, and guide cyber firms to work in Ethiopia, and business policies, and procedures which help to work as a cyber-security firm.

- **The demand for cybersecurity solutions**

This shows the number of needs or requests that would be provided to cyber firms to protect the critical organization asset of the client., and also, the innovative solutions, and products which are mainly produced based on customer demand.

- **Cybersecurity Awareness**

This is an assessment of awareness that helps to know the status of the cybersecurity level of the firm's management, employee, and society as a glance. If the management of the company does not have awareness of cybersecurity, it is hard to prepare cyber protection strategy so as it cannot protect its company from cyber incidents so to buy or to get any solution regarding cybersecurity the manager or the leader should have awareness of what he should do. In this case, the continuity of providing training, printable organization cyber awareness manuals, and other capacity programs can increase the awareness of all staff.

- **Number cybersecurity incidents**

These are any incidents that happened to business firms it can be attacked by a hacker or open hall that should be identified, and needs defense mechanism., and also, it includes cybercrime is a key issue when we consider cyber incidents related to cyber business growth because now a day's cyber-crime has been considered as a big business.

- **Number of Cyber Firms**

This shows the status of cyber firms in which firms are exit-early or not and about new startup cyber firms and existing cyber firms. which will help to show the increasing or decreasing status of the cyber firms. Identifying the unique challenge, they face from the government as well from the society on doing their business.

- **Cybersecurity Skilled Manpower**

This is one of the biggest concerns in which Cyber firms face for long they are challenged to get experts, and also a continuous skilled manpower turnover. This is a big concern in the cyber industry as well the government should support by including educational policy, and curriculum.

IJSER

## CHAPTER THREE

### RESEARCH METHODOLOGY

This chapter will discuss the method, and method of data collection this includes a study area, source of data, population size, and sampling technique, and size. It gives a summary of the Study Area, Target Population. Sample Size. Data collection instruments. Data types, and Data processing, and analysis.

#### 3.1 Research Setting

This purpose of the study is trying to indicate the relationship between those factors like cyber awareness. Cyber incidents, cyber firms, government business policy, and the growth of cyber business in the perception of those cyber actors. To achieve the main objective of the research; the researcher used a mixed approach both qualitative, and quantitative research design method to address the relationship between the above actors dependent, and independent variables. survey with semi-structured interviews and questionnaires employed.

#### 3.2 Study Area

The study focuses on ICT sectors like software companies, software, and hardware importers, and exporters, network companies, and Telecoms. Conditionally it may cover Internet café, maintenance, and electronic security device providers because currently, they play major roles indirectly in the Ethiopian cybersecurity market.

#### 3.2. Target Population

A total number of cyber firms are 814 those who are registered under the regulation of ministry of trade, and a total number of exporters of cyber software solutions are 19 according to the ministry of trade, and an industry source, and locally 160 active companies are working on software, and network development so a Total population size is 993 cyber business firms. But not all the firms are active out of 993 target population 553 of them are active, and the rest of them are idle the study focuses on active firms.

### 3.3. Sampling size

The researcher uses the following sample determination formulae which were developed by Taro Yamane (1967:886) to determine the sample size of the population. The rationale behind using this formula for calculating the sample size is – the formula gives a relatively large sample to be more representative of the population, in the formula confidence level is 95% with a margin of error 5% which is more acceptable in most Social Science studies.

$$*n=N/1+N(e)^2$$

where **n**=sample size

**N**= population size =993

**e**=Level of precision or sampling of Error which is +-5%

based on the above formulae the sampling size is calculated as follows

$$n=993/1+993(0.05)^2 = 993/2.3825 = \mathbf{232}$$

✎ The sample size is **232**

*Table 3.1 Sample Size Determination Table*

Research Techniques	Population	Sample Size	Methods
Questionnaire	993 cyber actors	232	simple random Sampling

### 3.4. Sampling technique

The study used a simple random sampling technique in coming up with the study's sample. The reason for using this technique is based on the respondent's accessibility, and willingness to fill the questionnaire.



### 3.5. Source of Data

The study will use two sources of data a Primary data which is a direct interview, and questioner with business owners, and CEOs, Directors or managers, and employees or experts who work in the cyber environment. Secondary data is requested from the ministry of trade, and industry, and Ministry of Innovation, and technology, in which they provide license for any Cyber related business, and also, other sources such as company websites, press releases, annual reports.

### 3.6. Data Collection Method

The study employed three methods during the process of data collection, and this was as follows;

Data collection is the process of gathering, and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes (Cooper & Schindler, 2008).

#### ☒ - Questionnaires:

The researcher administered questionnaires to selected employees, directors, owners, and Consultants from different firms as one means of data collection. The relevance of this was that the questionnaires were convenient and less time-consuming. With management staff who would not have time for an appointment, because of the coronavirus, it was hard to collect data physically so the researcher uses Google Docs Survey form for an online survey, and to notify them an email is used, and a questionnaire was sent to them which would easily be filled.

The questionnaire was incorporated a Likert scale of 5 measurements, with response options ranging from 'Highly disagreed (coded as 1) to 'Highly agreed (coded as 5) will be used for questions that better suit response to this type of format. To this end, the clear instruction presented to respondents is with the expectation to rate, and rank their perceptions from the given alternatives

- ☒ The secondary data source for the study. Those data is from Data ministry of innovation, and ministry of trade, and industry

### 3.7. Reliability Test

Reliability is defined as being fundamentally concerned with issues of consistency of measures. (Bryman, and Bell, 2003). According to Hair, et al., (2006), if  $\alpha$  is greater than 0.7, it means that it has high reliability, and if  $\alpha$  is smaller than 0.3, then it implies that there is low reliability. To meet the consistency reliability of the instrument, the questionnaire was distributed to 232 cyber actors of the cyber environment in Ethiopia, and Cronbach’s alpha was found to be for performance measure 0.683, the variables are approximately equal to 0.7 this shows the independent variable represents the dependent variable. The rest 31.7 percent are other variables not included in this study. Table 3.2 presents the consistency of measures based on the statistics tool.

Table 3.2: Reliability Test, and Statistics

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.683	.688	8

Source: Analysis Data from SPSS, 2020

Table 3.3: Reliability Test - Dependent Variable Cyber Business Growth

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.742	.741	4

Source: Analysis Data from SPSS, 2020

The above table shows that Cronbach’s Alpha with (0.742) indicates that 74.2% of the dependent variable questionnaires represent cyber business growth. The rest 25.8 percent are other variables not included in this study. Table 3.3 presents the consistency of measures based on statistics tool

### 3.8. Data Processing

Data processing includes coding and editing all the responses collected from the respondent which was edited with the view of checking for completeness, and accuracy to ensure that data is accurate

and consistent. Coding was done after editing which was done manually by the use of computers through SPSS.

### **3.9. Data Analysis**

The quantitative data were analyzed using both descriptive, and inferential statistics. Descriptive statistics were utilized for measures of central tendencies (Mean, Median, and Mode), and measures of dispersion (Variance, Standard Deviation, and Percentiles).

After collecting all the necessary data, these data were coded, and edited, analyzed, and rephrased to eliminate errors and ensure consistency. It involved categorizing, discussing, classifying, and summarizing the responses to each question in coding frames, basing on the various responses. This was intended to ease the tabulation work. It also helped to remove unwanted responses which would be considered insignificant.

Data collected from the respondents with the use of study instruments were classified into meaningful categories. This enabled the researcher to After collecting all the necessary data, these data were coded, and edited, analyzed, and rephrased to eliminate errors, and ensure consistency. It involved categorizing, discussing, classifying, and summarizing the responses to each question in coding frames, basing on the various responses. This was intended to ease the tabulation work. It also helped to remove unwanted responses which would be considered insignificant. Data collected from the respondents with the use of study instruments were classified into meaningful categories. This enabled the researcher to bring out essential patterns from the data that would organize the presentation. Data were entered into a computer and analyzed with the use of statistical packages for social science (SPSS). Finally, a research report was written from the analyzed data in which conclusions and recommendations were made.

### **3.10. Data Presentation**

The researcher presented data got from the primary, and secondary sources using statistical package for social science (SPSS Version 25) software, and the result was presented in tables for easy interpretation.

### **3.11. Ethical Consideration**

Before the research was conducted on cyber issues, the researcher informed the participants of the study about the objectives of the study and was consciously consider ethical issues in seeking consent, avoiding deception, maintaining confidentiality, respecting the privacy, and protecting the anonymity of all respondents. A researcher must consider these points because the law of ethics on research condemns researching without the consensus of the respondents for the above-listed reasons.

IJSER

## CHAPTER FOUR

### DATA ANALYSIS, and INTERPRETATION

#### 4.1 Introduction

This chapter presents the data presentation, interpretation, and analysis of the study. The first section is all about the response rate of the respondents. The chapter further presents responses concerning the study objectives which include; findings on how awareness, legislation, skilled manpower, the increase in cyber firms, government business policy, and cyber incidents affect cyber business growth and also find out the relationship between those factors, and cyber business growth.

To achieve the main objective of the research a total of 232 questionnaires were distributed through google docs, it is distributed to 232 respondents with experts, owners/CEOs, Consultants, and directors of different firms with different ages, and gender. Out of these questionnaires, 191 responses were valid with a complete answer. Therefore, only 191 questionnaires were used for further analysis.

*Table 4.2 Response Rate of Respondents*

Profile of Respondents Statistics						
Profile	Gender of Respondent	Age of Respondent	Educational Level of Respondents	Work experience of the Respondents	Occupation	
N	191	191	191	191	191	191
Missing	0	0	0	0	0	0
Mean	1.22	2.18	2.45	3.33	2.53	
Median	1.00	2.00	2.00	4.00	3.00	
Std. Deviation	.415	.659	.568	.821	.978	
Percentiles	25	1.00	2.00	2.00	3.00	2.00
	50	1.00	2.00	2.00	4.00	3.00
	75	1.00	3.00	3.00	4.00	3.00

**Source: Primary data 2020**

## 4.2 Profiles of Respondents

The demographic characteristics of the respondents include Gender, Age, Level of education, Service year, and Occupation about their views, and perceptions about the factors affecting cyber business growth in Ethiopia. Concerning the background characteristics of the respondents, several variables were investigated. The researcher regarded investigating the background variables about the respondents a necessary undertaking because it helped him to know the extent to which the respondents possess an acquaintance with the study area as well as the variables under study. The study involved respondents of varying characteristics which enabled the researcher to get sufficient information on the study variables as follows.

*Table 4.1 Profile of the respondent*

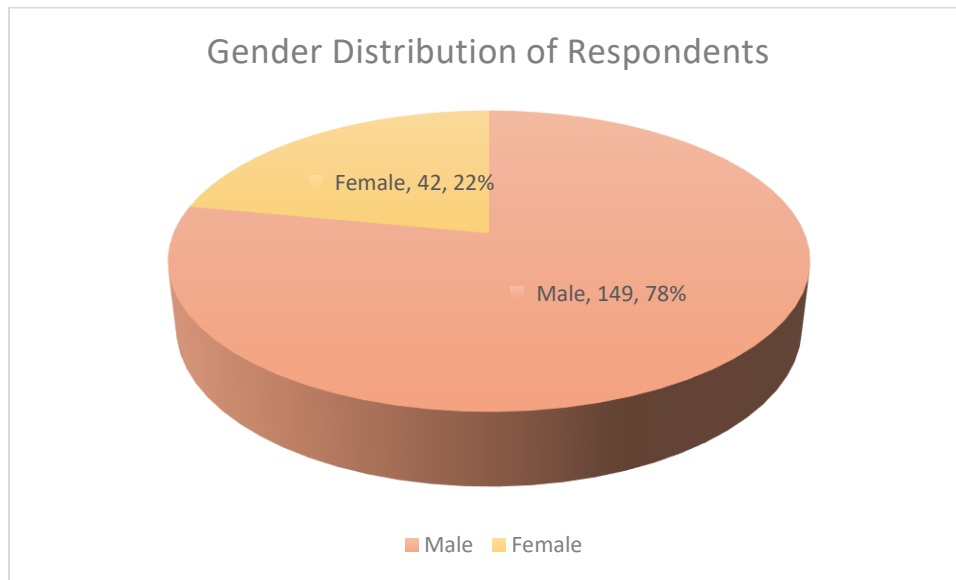
Statistics						
Profiles		Gender of the Respondent	Age of the Respondent	Level of Education of respondent	Work experience of the Respondents	Occupation
N	Valid	191	191	191	191	191
	Missing	0	0	0	0	0

**Source: Primary data 2020**

### 4.2.1 Gender of the Respondent

The researcher also looked at the Gender category of the respondent to link the Gender of respondents with factors affecting cyber business growth.

Figure 2: Gender of Respondents



**Source: Primary data 2020**

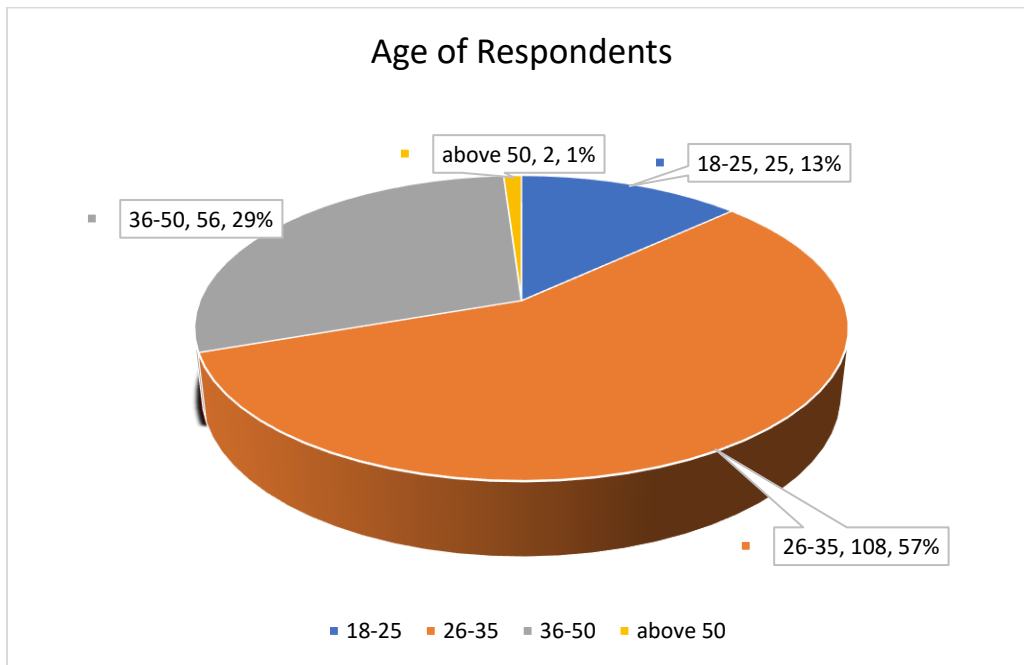
According to the study findings from the total of 191 respondents, 149 (78%) of them are male, and 42 (22%) of them are female this shows most of the respondents are male, and are interested to support the improvement of cyber business in Ethiopia so that they are eager to show the challenges, and the factors affecting cyber business growth.

#### 4.2.2 Age of the Respondent

According to the study, most of the respondents are the age above 25-year-old. In this case, the researcher also looked at the age category of the respondent to link the age with factors affecting cyber business growth.

The findings in table bellow indicate that majority of the respondents were in age category 26-35, and 36-50 years with 56.5%, and 29.3% respectively. This was attributed to the fact that most young employees are eager to improve and contribute to the improvement of cyber business growth.

Figure 3: Age of Respondents



Source: Primary data 2020

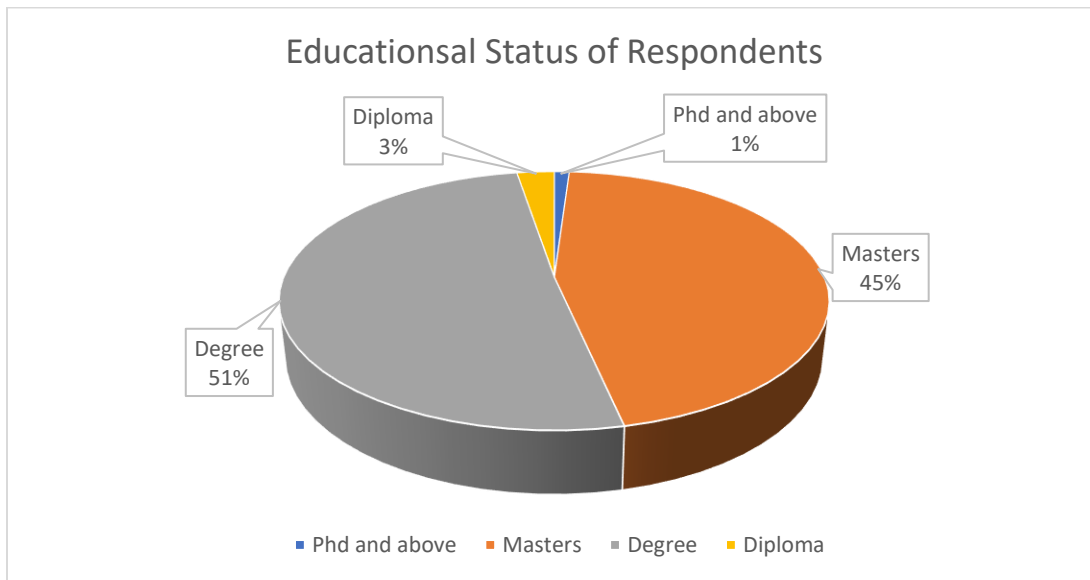
### 4.2.3 Level of Education of the Respondents

The researcher also looked at the Level of Education of the respondents to link the Level of Education with factors affecting cyber business growth.

The findings in the table below indicate that majority of the respondents were in Level Level of Education of category Degree, and Masters with 50.8%, and 45.5% respectively. This was attributed to the fact that most business owners are Degree holders, and master's level. This respondent has highly contributed to cyber business growth.



Figure 4: Educational Status of Respondents

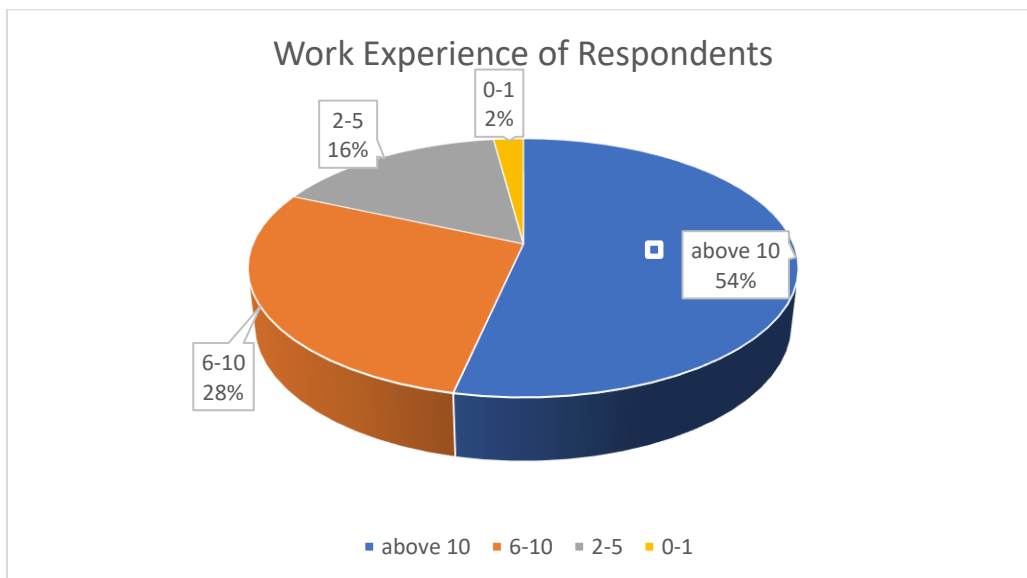


Source: Primary data 2020

#### 4.2.4 Work experience of the Respondents

The researcher also looked at the Work Experience of the respondent to link the work experience of respondents with factors affecting cyber business growth.

Figure 5: Work Experience of Respondents



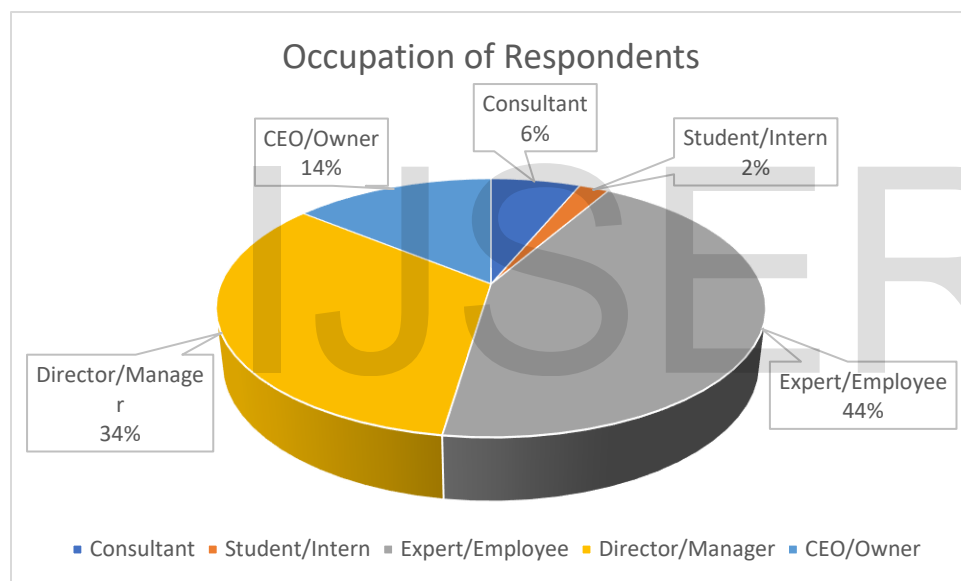
Source: Primary data 2020

The above findings indicate that majority of the respondents were in Level of the category above 10years, and 6-10, and 102 respondents with 53.4%, and 54 respondents with 28.3% respectively. This was attributed to the fact that most of the respondents are well experienced, and know the fact that the major challenges, and factors affecting cyber business. This makes them easily explain the factors that affect cyber business growth.

#### 4.2.5 Occupation of the Respondents

The researcher also looked at the Occupation of the respondent to link the Occupation of respondents with factors affecting cyber business growth.

Figure 6: Occupation of Respondents



Source: Primary data 2020

The above findings indicate that majority of the respondents were in Level of category Experts, and Directors, and 84 respondents with 44%, and 64 respondents with 33.5% respectively. This was attributed to the fact that most of the cyber experts and cyber Directors are eager to improve and contribute to the improvement of cyber business growth. They can easily explain the factors that affect cyber business growth.

### 4.3 Results, and Interpretations

#### 4.3.1 Analysis of Cybersecurity awareness

The following table shows an analysis of cyber awareness

*Table 4.2 Analysis of Cyber awareness*

Profile of Respondents Statistics							
Cybersecurity Awareness	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
As an organization you provide or you get continuous, and planned security awareness training.	12	58	40	48	33	3.16	1.21
Cyber-security is considered a Core component of the organization	4	23	20	50	94	4.08	1.12
You have awareness of key organization information assets	12	2	32	74	71	3.99	1.07
You have enough knowledge on how to protect your computer, mobile, and tablets from attack.	2	7	25	81	76	4.16	0.86
You have enough knowledge about security solutions that are provided by cybersecurity firms	30	19	39	91	12	3.19	1.19

**Source primary data, survey 2020**

As it is presented in the above table, it is clear that out of 191 respondents (30.4%) have disagreed that they do not provide cyber awareness training for their employees or they had no training at all. Also, (25.1%) of the respondents had agreed, and (17.1%) are strongly agreed that there is a cybersecurity awareness program in their organization.

Thus, the research had revealed that cyber awareness is agreed by (42.2%) of the respondents, and disagreed by (36.7%) of the respondents. This finding implies that most firms do not provide enough awareness for their employees so that they have a significant contribution to the cyber business.

**4.3.2 Analysis of Cyber Legislation**

*Table 4.3 Analysis of Cyber Legislation*

Profile of Respondents Statistics

Cyber Legislation	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
There is the cyber policy, and Legislation Nationally to help guide government or private firms regarding cybersecurity solutions	3	39	85	42	22	3.21	0.95
There is National Cyber-crime Law, and regulation in Ethiopia	4	6	78	90	13	3.53	0.75
There is a Cybersecurity Requirement standard which guides any security specification implementation of any information systems	4	31	60	64	32	3.47	1.02
Nationally there is cybersecurity Stated Standard Framework Like NIST	6	46	91	37	11	3.01	0.89

Source primary data, survey 2020

From The above table, it is clear that out of 191 respondents (20.4%) have disagreed, and (1.6%) strongly disagreed that there is national cyber guideline, and standard that should be followed, and leads those solutions that will be implemented in any institutions in Ethiopia. In contrast (22%), and (11.5%) of respondents agreed, and strongly agreed there are government guidelines and policy support standards that will be followed by solution providers.

Thus, the research had revealed that the cyber national cyber guideline is in place to support guide solution demand and implementation which is agreed by (33.5%) of the respondents, and disagreed by (22%) of the respondents. This finding implies that the government provides, and avail the necessary guideline, and standard, but in another way (44.5%) of respondents have no idea that there is a cybersecurity guideline, and the procedure is in place.

Table 4.4 Analysis of Cyber Solution Demand

**Profile of Respondents Statistics**

Cybersecurity Solution Demand	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
There is a continuous demand on cyber-related solutions on your organization	3	7	52	73	56	3.90	0.92
Cyber firms provide solutions as per expected or demanded quality standard	2	33	102	39	15	3.17	0.84
Demand of cyber solution increase in national level	2	7	24	75	83	4.20	0.87

**Source primary data, survey 2020**

The above table, it is clear that out of 191 respondents (3.7%) have disagreed, and (1%) strongly disagreed that there is an increase in cybersecurity solution demand. In contrast (39.3%), and (43.5%) of respondents agree, and strongly agree by the concept there is, an increase in the number of cybersecurity solution demand that will be provided from respondents.

Thus, the research had revealed that the cyber solution is an increase in number to help grow the cyber business, and which is agreed by a total of (82.8%) of the respondents, and disagreed by a total of (4.7%) of the respondents. This finding implies that cyber solution demand is tremendously increasing thus the cyber business will hopefully grow in a short period.

### 4.3.3 Analysis of Cyber Skilled Manpower

Table 4.5 Analysis of Cyber Skilled manpower

Profile of Respondents Statistics							
Cyber Skilled Manpower	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
There are experts Turnover on your organization who work on cyber-related functions	6	34	83	33	35	3.3	1.06
You have certified professional cyber experts on your organization	24	28	23	73	43	3.43	1.32
It is easy to get and recruit skilled manpower regarding information security	36	94	30	19	12	2.36	1.09
Government education policy helps to easily available the information security skilled manpower	42	76	56	11	6	2.28	0.97

**Source primary data, survey 2020**

The above table, it is clear that out of 191 respondents (49.2%) have disagreed, and (18.8%) strongly disagreed that there is skilled manpower regarding cybersecurity. In contrast (9.9%), and (6.3%) of respondents agreed, and strongly agreed there is skilled manpower that is provided by respondents.

Thus, the research had revealed that the lack of skilled manpower exists regarding cybersecurity, and this has a big factor to help grow the cyber business, and which is disagreed by a total of (68%) of the respondents, and agreed by a total of (16.2%) of the respondents. This finding implies that lack of cyber skilled manpower has existed, and it has a big impact on the growth of the cyber business.

### 4.3.4 Analysis of Cyber Firms

Table 4.6: Analysis of Cybersecurity Firms

Profile of Respondents Statistics							
Cyber Firms	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
Cybersecurity firms are increasing in number	5	33	59	82	12	3.33	0.92
most new cyber firms are exit/terminate early	1	4	102	65	19	3.51	0.72
Most of the firms have international standards and provide the expected solution or user need	7	44	87	40	13	3.04	0.928

**Source primary data, survey 2020**

As it is presented in the above table, it is clear that out of 191 respondents (17.3%) have disagreed, and (6.2%) are strongly disagreed that cyber firms are increasing in number. but, (42.9%) of the respondents had agreed, and (6.3%) are strongly agreed that there is an increasing number of cyber firms.

Thus, the research had revealed that the cyber firms are increasing in number is agreed by a total of (49.2%) of the respondents, and disagreed by (23.5%) of the respondents. This finding has an implication that there is an increase in the number of new cyber firms this has a direct impact so that they have a significant contribution to cyber business growth.

**4.3.5 Analysis of Government business policy**

Table 4.7: Analysis of Government Business Policy

Profile of Respondents Statistics							
Government business policy	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
There is Support from Government through policy, and regulation to help improve the cyber environment	15	54	73	45	4	2.84	0.92
Appropriate international and local business policy is in place to start a cyber business	15	39	90	41	6	2.92	0.92
The government provides Incentive factor-like Tax exemption, providing the working place, and other facilities	18	66	83	22	2	2.60	0.85
It is easy to start and exit the cyber business in Ethiopia	19	75	81	11	5	2.52	0.85

**Source primary data, survey 2020**

In the above table, it is clear that out of 191 respondents (39.3%) have disagreed, and (9.9%) are strongly disagreed that starting, and exiting the bureaucracy of cyber firms in Ethiopia is easy. but, (5.8%) of the respondents had agreed, and (2.6%) are strongly agreed that it is easy to start, and exiting the cyber business in Ethiopia.

Thus, the research had shown that the starting new cyber firms, and exiting cyber firms are difficult, and from the respondents those who agreed by a total of (8.4%) of the respondents, and disagreed by (49.2%) of the respondents. This finding implies that it is so hard to start, and exit the cyber business in Ethiopia, and also it shows it is difficult to do cyber business in Ethiopia so that the bureaucracy government business policy has a significant contribution to cyber business growth.

**4.3.6 Analysis of Cyber Incident**



Table 4.8: Analysis of Cyber incidents

Profile of Respondents Statistics							
Cyber Incidents	1	2	3	4	5	Mean	Std. Deviation
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree		
	Freq	Freq	Freq	Freq	Freq		
you are facing continuous personal cyber-attack or incident on your mobile, and personal devices	15	79	46	44	7	2.73	1.01
Frequently cyber-attack happened on organization information assets	13	33	52	79	22	3.29	1.09
You have enough information about incidents and cyber-attack on your organization	5	22	51	70	43	3.65	1.035

**Source primary data, survey 2020**

The above table depicts that, it is clear that out of 191 respondents (17.3%) have disagreed, and (6.8%) are strongly disagreed that frequently cyber incidents are happening in their organization. but, (37.2%) of the respondents had agreed, and (11.5%) are strongly agreed that there is a continues cyber incident on their organization.

Thus, the research had shown that there is an increase in the number of cyber incidents in firms from the respondents who agreed by a total of (48.7%) of the respondents and disagreed by (24.1%) of the respondents. This finding implies that the increasing number of cyber incidents is getting worse so that if the cyber incident increase it has demand for a cyber solution is increase this directly affects cyber business growth.

**4.3.7 Analysis based on the mean, and standard deviation**

Table 4.9: Results of Descriptive analysis

Discriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Cyber_Security_Awareness	191	1.00	5.00	3.7103	.67005
Cyber_Security_Legislation	191	1.25	5.00	3.3050	.60010
Solution_Demand	191	1.67	5.00	3.7574	.63699
Skilled_Manpower	191	1.25	4.50	2.8429	.56388
Cyber_Firms	191	1.67	5.00	3.2932	.57848
Government_Business_Policy	191	1.00	5.00	2.7186	.61905
Cyber_Incident	191	2.00	5.00	3.2251	.67792
Valid N (listwise)	191				

**Source: Author’s Survey Analysis, 2020.**

According to the above table, the highest mean value (3.75) shows that most of the respondents believed that the increasing number of solution demands has a better effect on cyber business growth followed by cybersecurity awareness with the mean (3.71). This implies that when firms need to be secure, and the more the demand more cyber business growth, and also the more the people become aware of the security the more they need to be secure thus, the higher the business growth. Furthermore, cyber business growth highly affected and related to its demand, and cybersecurity awareness. However, cybersecurity legislation with a mean of (3.30), and cyber firms with a mean (3.29), and cyber incidents with a mean value of (3.22) moderately affect the cyber business growth. This indicates that cyber business growth can also be affected by the strength of its legislation, existence, and several cyber firms, and the existence of cyber incidents respectively. Thus, the strongest the legislation, the existence of incident, and the increasing number of cyber firms increase cyber business growth. The remaining skilled manpower, and government business policy with a mean value (2.84), and (2.71) respectively affect the cyber

business growth weakly. This implies that the cyber business growth, and skilled manpower, government business policy weakly related.

#### 4.4 Results of Correlation Analysis

The following result indicates that the relationship between those factors that affect business growth, and cyber business growth. Besides, a correlation coefficient enables us to quantify the strength of the linear relationship between numerical variables. This coefficient (usually represented by the letter  $r$ ) can take on any value between +1, and -1. A value of +1 represents a perfect positive correlation. This means that the two variables are precisely related, and that, as values of one variable increase, the values of another variable will increase. By contrast, a value of -1 represents a perfect negative correlation. Again, this means that the two variables are precisely related; however, as values of one variable increase those of the other decrease. Correlation coefficients between +1, and -1 represent weaker positive and negative correlations, a value of 0 meaning the variables are perfectly independent or there is no relationship between the variables.

Table 4.9: Results of Correlation Matrix

		Correlations							
Factors		Cyber_ Busine ss_Gro wth	Cyber_ Securit y_Awa reness	Cyber_ Securit y_Legi slation	Solutio n_Dem and	Skille d_Ma npowe r	Cyber_ Firms	Gover nment _Busin ess_Po licy	Cyber_ Incede nt
Cyber_Business _Growth	Pearson Correlation	1	.233**	.273**	.421**	.120	.362**	.469**	-.126
	Sig. (2-tailed)		.001	.000	.000	.099	.000	.000	.082
	N	191	191	191	191	191	191	191	191
Cyber_Securit y_Awareness	Pearson Correlation	.233**	1	.401**	.550**	.232**	.096	.170*	.243**

	Sig. (2-tailed)	.001		.000	.000	.001	.187	.019	.001
	N	191	191	191	191	191	191	191	191
Cyber_Security_Legislation	Pearson Correlation	.273**	.401**	1	.516**	.203**	.195**	.338**	.202**
	Sig. (2-tailed)	.000	.000		.000	.005	.007	.000	.005
	N	191	191	191	191	191	191	191	191
Solution_Demand_and	Pearson Correlation	.421**	.550**	.516**	1	.228**	.246**	.238**	.080
	Sig. (2-tailed)	.000	.000	.000		.002	.001	.001	.273
	N	191	191	191	191	191	191	191	191
Skilled_Manpower	Pearson Correlation	.120	.232**	.203**	.228**	1	.287**	.310**	.012
	Sig. (2-tailed)	.099	.001	.005	.002		.000	.000	.874
	N	191	191	191	191	191	191	191	191
Cyber_Firms	Pearson Correlation	.362**	.096	.195**	.246**	.287**	1	.158*	-.099
	Sig. (2-tailed)	.000	.187	.007	.001	.000		.029	.173
	N	191	191	191	191	191	191	191	191
Government_Business_Policy	Pearson Correlation	.469**	.170*	.338**	.238**	.310**	.158*	1	-.311**
	Sig. (2-tailed)	.000	.019	.000	.001	.000	.029		.000
	N	191	191	191	191	191	191	191	191
Cyber_Incident	Pearson Correlation	-.126	.243**	.202**	.080	.012	-.099	-.311**	1
	Sig. (2-tailed)	.082	.001	.005	.273	.874	.173	.000	

N	191	191	191	191	191	191	191	191
---	-----	-----	-----	-----	-----	-----	-----	-----

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

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

**Source: Author’s Survey Analysis, 2020.**

As shown in Table 4.9 Pearson Correlations Matrix has been concluded as follows: there is a statistically significant, and strong positive relationship between cyber business growth, and Cyber\_Security\_Awareness ( $r= 0.233, p <0.01$ ), Cyber\_Security\_Legislation ( $r = 0.273, p <0.01$ ), Solution\_Demand ( $r= 0.421, p <0.01$ ), Skilled\_Manpower ( $r= 0.120, p <0.01$ ), Cyber\_Firms ( $r= 0.362, p <0.01$ ), Government\_Business\_Policy ( $r= 0.469, p <0.01$ ), and negative relationship with Cyber\_Incident ( $r= -0.126, p <0.01$ ).

In the case of impact, the availability of Cybersecurity legislation, the capacity of cyber Awareness, the increase in the number of cyber firms, the availability of skilled manpower, the improvement of government business policy can positively affect cyber business growth. In contrast, the only factor that affects negatively is cyber incidents negatively so cyber incidents, and cyber business growth are in the opposite direction.

**4.5 Results of Regression Analysis**

Regression analysis is a technique used in statistics for investigating, and modeling the relationship between variables (Douglas Montgomery, Peck, & Vinning, 2012).

The following table shows that the Measure of Quality of Prediction value for Cyber Business Growth R can be considered to be one measure of the quality of the prediction of cyber business growth. In this study  $R = 0.628^a$  this indicates a good level of prediction.

*Table 4.10: Measure of Quality of Prediction*

Model Summary										
Model	R	R Square	Adjusted R Square	Std. Error	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	

1	.628 <sup>a</sup>	.395	.372	.47792	.395	17.052	7	183	.000	2.253
---	-------------------	------	------	--------	------	--------	---	-----	------	-------

a. Predictors: (Constant), Cyber\_Incident, Skilled\_Manpower, Solution\_Demand, Cyber\_Firms, Government\_Business\_Policy, Cyber\_Security\_Awareness, Cyber\_Security\_Legislation

b. Dependent Variable: Cyber\_Business\_Growth

**Source: Author’s Survey Analysis, compiled from SPSS 2020.**

As shown in table 4.10 the R<sup>2</sup>, and adjusted R<sup>2</sup> values of the model: 0.395, and 0.372 respectively, both indicated that there was a moderate degree of goodness of fit of the regression model. It also means that 39.5 percent of the variance in the dependent variable (cyber business growth) can be explained by the regression model. The rest 60.5 percent are other variables not included in this study.

The *F*-ratio in the ANOVA table (see below) tests whether the overall regression model is a good fit for the data. The table shows that the independent variables statistically significant predict the cyber business growth,  $F(7, 183) = 17.052, p < .0005$  (i.e., the regression model is a good fit of the data).

Table 4.11 ANOVA

ANOVA <sup>a</sup>						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	27.264	7	3.895	17.052	.000 <sup>b</sup>
	Residual	41.799	183	.228		
	Total	69.062	190			

a. Dependent Variable: Cyber\_Business\_Growth

b. Predictors: (Constant), Cyber\_Incident, Skilled\_Manpower, Solution\_Demand, Cyber\_Firms, Government\_Business\_Policy, Cyber\_Security\_Awareness, Cyber\_Security\_Legislation

**Source: Author’s Survey Analysis, 2020.**

The ANOVA test of the above model which species cyber business growth as a function of Cyber Incident, Skilled Manpower, Solution Demand, Cyber\_Firms, Government Business Policy,

Cyber\_Security\_Awareness, Cyber\_Security\_Legislation. ANOVA tells the overall goodness of fit of the model. F-statistic of the model is 17.052 which is quite good and entails that model is a good fit at a 1% level of significance. The *F*-test result was 17.052 with significance ('Sig.') of .000. This means that the probability of these results occurring by chance was less than 0.0005. Therefore, the significant relationship was present between cyber business growth, and Cyber Incident, Skilled Manpower, Solution Demand, Cyber\_Firms, Government Business Policy, Cyber\_Security\_Awareness, Cyber\_Security\_Legislation.

This is a test for the statistical significance of each of the factors. This tests whether the unstandardized (or standardized) coefficients are equal to 0 (zero) in the population. If  $p < .05$ , we can conclude that the coefficients are statistically significantly different to 0 (zero). The *t*-value and corresponding *p*-value are located in the "t", and "Sig." columns, respectively, as highlighted below:

Table 4.12: Regression Result for Cyber Business growth

		Coefficients								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	.645	.351		1.839	.068	-.047	1.338		
	Cyber_Security_Awareness	.021	.065	.023	.315	.753	-.108	.149	.631	1.585
	Cyber_Security_Legislation	-.063	.074	-.062	-.847	.398	-.208	.083	.611	1.635
	Solution_Demand	.290	.072	.306	4.008	.000	.147	.432	.568	1.761
	Skilled_Manpower	-.164	.068	-.153	-2.399	.017	-.298	-.029	.811	1.233
	Cyber_Firms	.287	.065	.276	4.442	.000	.160	.415	.859	1.165
	Government_Business_Policy	.412	.068	.423	6.040	.000	.277	.546	.675	1.480
	Cyber_Incident	.015	.060	.017	.254	.800	-.102	.133	.737	1.356

a. Dependent Variable: Cyber\_Business\_Growth

**Source: Author's Survey Analysis, 2020.**

In the above table we can see the p-value <0.05 are solution demand, cyber firms, skilled manpower, government business policy. So, from the table we can conclude that solution demand, cyber firms, skilled manpower, government business policy have a statistically significant relationship with cyber business growth, and the rest cybersecurity awareness, cybersecurity legislation, and the cyber incident is their p-value is > 0.05.

*Table 4.13: Residuals Statistics of Cyber Business Growth*

Residuals Statistics					
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.0877	4.3319	3.2513	.37880	191
Residual	-1.67022	1.51842	.00000	.46903	191
Std. Predicted Value	-3.072	2.853	.000	1.000	191
Std. Residual	-3.495	3.177	.000	.981	191

a. Dependent Variable: Cyber\_Business\_Growth

**Source: Author's Survey Analysis, 2020.**



Figure 7: Scatterplot of Frequency Distribution

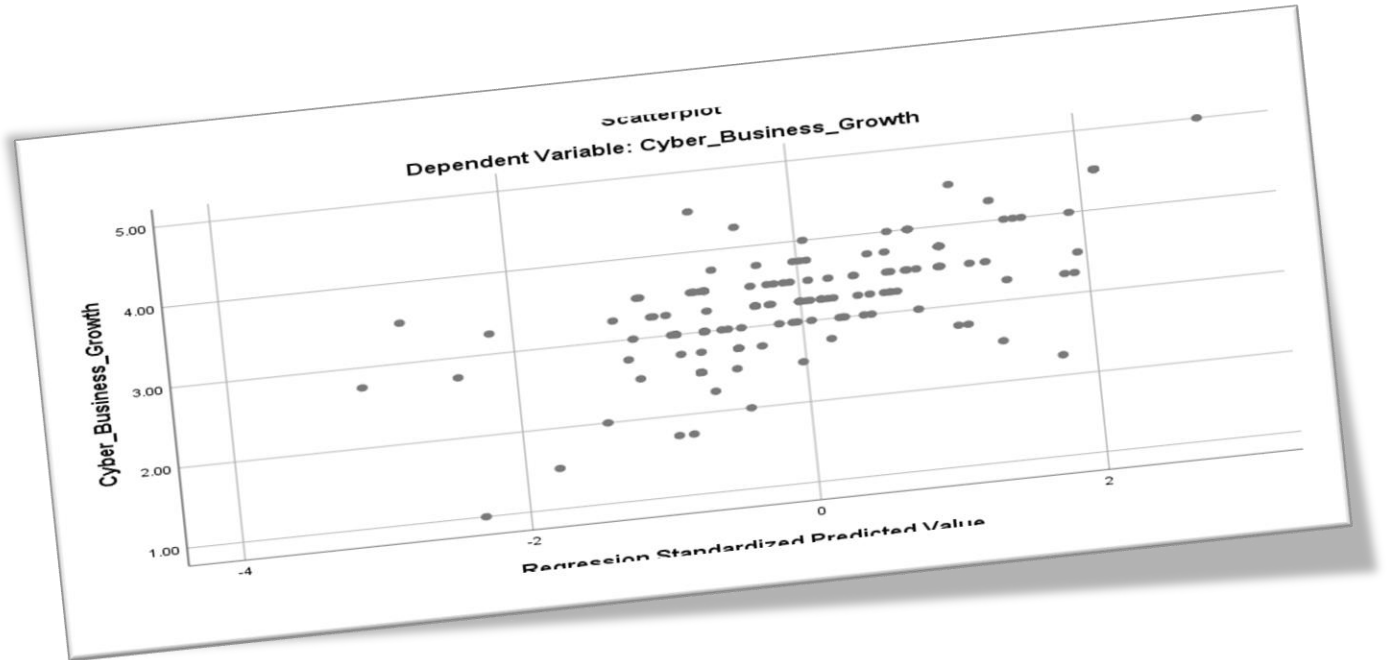
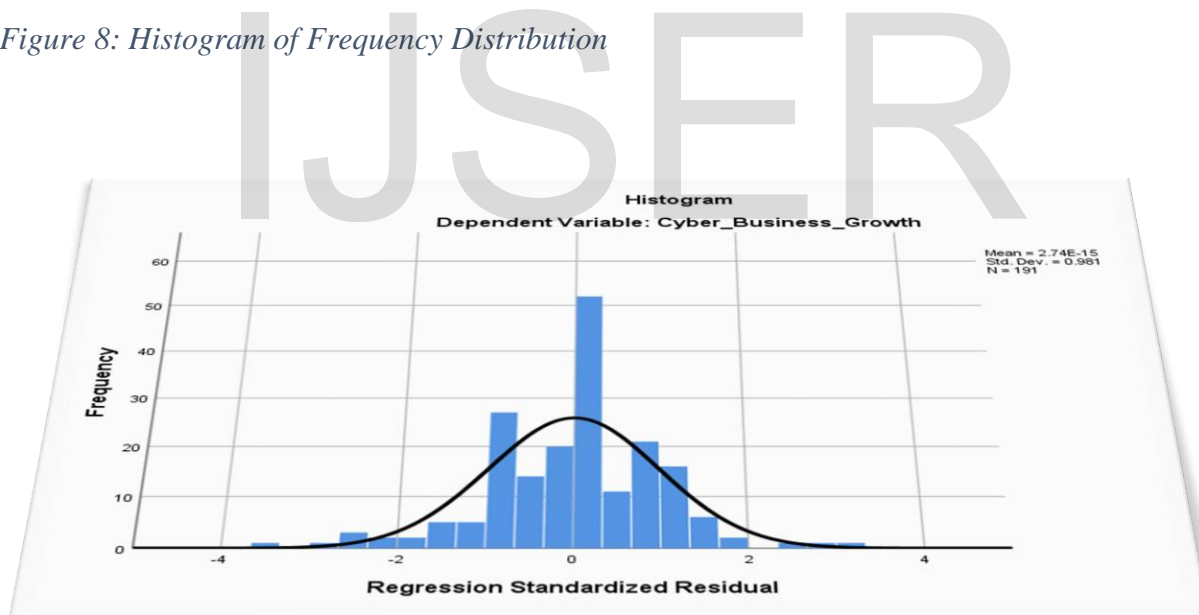


Figure 8: Histogram of Frequency Distribution



The regression of cybersecurity awareness (CSA), Cyber Legislations (CL), Cyber Solution Demand (CSD), Government Business Policy (GBP), Cybersecurity Incident (CSI), Cyber Skilled Manpower (CSM), and Cyber Firms (CF) on Cyber Business Growth (Y) is considered. Thus:

$$Y = a + b_1CSA + b_2CL + b_3CSD + b_4GBP + b_5CSI + b_6CSM + b_7CF.$$

The empirical result presented in Table 11 reveals that except cybersecurity incidents all proof are significant determinants of cyber business growth values paid by respondents of those cyber actors in different cyber firms of Ethiopia. In the consideration of the entire variables fitted into the model, R<sup>2</sup> (0.395) shows that about 39.5% of the variation in business growth are jointly accounted for by the variables. The standard coefficients (Beta) give a picture of the relative importance or influence of the independent variables on the cyber business growth. The higher the magnitude of Beta, the more the influence in of the variable:

$$\text{Cyber Business Growth} = \alpha + \beta_1(\text{CSA}) + \beta_2(\text{CL}) + \beta_3(\text{SD}) + \beta_4(\text{SM}) + \beta_5(\text{CF}) + \beta_6(\text{GBP}) + \beta_7(\text{CI}) + e$$

$$(Y) = 0.645 + 0.023(\text{CSA}) + (-0.062)(\text{CL}) + 0.306(\text{SD}) + (-0.153)(\text{SM}) + 0.276(\text{CF}) + 0.423(\text{GBP}) + 0.017(\text{CI}) + \text{Error}$$

The empirical results of the multiple regression models are presented in Table 16. It shows that if there is no Government Business policy, cyber solution demand is the most determining variable of Cyber Business growth. This is followed by an increasing number of cyber firms. Next to this in order of influence is Cyber Awareness, Cyber Incident/Crime, skilled manpower, and Cyber Legislation respectively.

From the empirical result of the stepwise regression presented in Table 16, six of the seven (7) factors are very crucial for the determination of Cyber Business growths by respondents of the cyber actor in different firms.

The most crucial is Government Business Policy with a regression coefficient of 0.412, and the second most important is solution demand with a 0.290 regression coefficient. Those factors put together contributed 37.2% in the determination of cyber business growth in Ethiopia. These seven factors are cyber firms, cyber legislation, awareness, solution demand, government business policy, Skilled manpower, and cyber incident. It can be concluded that respondents valued the government business policy, and solution demand plays a vital role in the growth.

Therefore, based on the coefficients of the dependent variable ( $\beta$  sign) all the hypotheses projected in this research are acceptable because six of the hypotheses stated the positive relationship with the dependent variable is met, and the only cyber incident resulted in a negative relationship. In

addition to this, all independent variables are significantly contributed to the Cyber Business growth at ( $p < 0.01$ ) level of confidence.

#### 4.6 Hypotheses Test

The regression analysis, which results are presented in the above table a more complete, and perfect examination of the research hypothesis. Therefore, the regression results obtained from the model were utilized to test these hypotheses. As can be seen in the table above the p-value for solution demand, skilled manpower, increase in cyber firms, and government business policy variables are statistically significant at ( $p < 0.01$ ) which suggests strong support for those four hypotheses. The following hypothesis tests were conducted based on the regression results of the cyber business growth dimensions obtained from the regression output.

*Table 4.14 Hypothesis Testing/Accepted or Rejected*

Hypothesis	Accepted/ Rejected
⊗ H01: Cybersecurity awareness does not have a significant effect on the growth of cyber business growth.	✓
⊗ Ho2: Cybersecurity Legislations does not have a significant effect on the growth of cyber business growth	✓
⊗ Ho5: The demand for cybersecurity solutions does not have a significant effect on the growth of the cybersecurity business.	x
⊗ Ho7: Cybersecurity Skilled Manpower does not have a significant effect on the growth of cybersecurity business.	x
⊗ Ho4: Number of cyber firms does not have a significant effect on the growth of the cybersecurity business.	x
⊗ Ho6: Government Business Policy does not have a significant effect on the growth of the cybersecurity business.	x

---

✎ Ho3: Number of cyber incidents does not have a significant effect on the growth of the cybersecurity business.	✓
--	---

---

✎ Cyber Solution Demand, and Cyber business growth

The regression output result also supports this hypothesis with significantly correlated variables with the level of significance ( $p < 0.01$ ), and the positively related coefficients ( $\beta = 0.290$ , and  $t = 4.008$ ) contribute to the cyber business growth. The regression coefficients 0.290 shows that any increase in the variable solution demand of cyber solution for one unit of value will raise the growth of cyber business growth to 0.290 units of value or 29% assuming other variables are constant.

✎ Cyber Business Firms, and Cyber Business growth

Researchers have demonstrated that increasing cyber business firms' dimensions of factors affecting cyber business growth has a positive impact on cyber business growth.

The regression output result also supports this hypothesis with significantly correlated variables with the level of significance ( $p < 0.01$ ), and the positively related coefficients ( $\beta = 0.287$ , and  $t = 4.442$ ) contribute for the business growth. The regression coefficients 0.287 shows that any increase in the variable cyber firms of the cyber sector for one unit of value will raise the growth of the cyber business to 0.287 units of value or 28.7% assuming other variables are constant.

✎ Cyber Skilled Manpower, and Cyber business growth

The cyber skilled manpower becomes highly growing in demand, according to the tangible facts of the study in this sector, it can be said that there is a positive, and significant influence of skilled manpower on cyber business growth. Similarly, many researchers have found a meaningful influence in this sense "There will be 3.5 million unfilled cybersecurity jobs by 2021", and this shows the sector is growing and is highly impacted by skilled manpower (UNCTAD, 2020).

The regression output result also supports this hypothesis with significantly correlated variables with the level of significance ( $p < 0.01$ ), and the positively related coefficients ( $\beta = -0.164$ , and  $t = -2.399$ ) contributes for the business growth. The regression coefficients 0.164 shows that any decrease in the variable skilled manpower of the cyber sector for one unit of value will decrease the growth of cyber business growth to 0.164 units of value or 16.4% assuming other variables are constant.

### ☞ Government business policy, and Cyber business growth

The government business policy has highly impacted the growth of the cyber business. This is one of the most challenges every startup faces, according to the tangible facts of the study in this sector, it can be said that there is a negative and significant influence of government business policy on cyber business growth.

The regression output result also supports this hypothesis with significantly correlated variables with the level of significance ( $\rho < 0.01$ ), and the positively related coefficients ( $\beta = 0.412$ , and  $t = -6.040$ ) contribute to the business growth. The regression coefficients 0.412 shows that any increase in the variable Government Business policy of the cyber sector for one unit of value will increase the growth of cyber business growth to 0.412 units of value or 41.2% assuming other variables are constant.

### ☞ The Relationship between Cyber Legislation, and Cyber business growth

This is one of the most challenging issue the government must work, according to the tangible facts of the study in this sector, it can be said that there is a negative and significant influence of cyber legislation on cyber business growth.

The regression output result also supports this hypothesis with significantly correlated variables with the level of significance ( $\rho < 0.01$ ), and the negatively related coefficients ( $\beta = -0.063$ , and  $t = -0.847$ ) contributes for the business growth. The regression coefficients -0.063 shows that any decrease in the variable cyber legislation of the cyber sector, for one unit of value it decreases the growth of cyber business growth to -0.063 units of value or 6.3% assuming other variables are constant.

## Chapter Five

### Summary, Conclusion, and Recommendation

This chapter deals with addressing the objective of the study is as of factors affecting cyber business growth., and to find out the relationship of those identified list of variables as factors affecting the cyber business growth. Furthermore, this chapter summarizes findings conclusions, and finally state recommendations.

#### 5.1 Summary, and major findings

Based on the objective of the study, the researcher summarized the major findings as follows.

- ✎ The statistical description of factors affecting the growth (see table 4.9) where it has found that major driver for growth is based on Mean, and standard deviation are cyber solution demand, and cyber awareness (with the highest mean scores, i.e.  $M = 3.7574$ ,  $SD = .63699$ , and  $M = 3.7103$ ,  $SD = .67005$  respectively) to be the most dominant factor of the cyber growth evident to a considerable extent for awareness, followed by Cybersecurity Legislation ( $M = 3.3050$   $SD = 0.60010$ ), Cyber Firms ( $M = 3.2932$ ,  $SD = 0.57848$ ), and Cyber Incident ( $M = 3.2251$ ,  $SD = 0.6792$ ) which was rated as moderately impact the growth. Cyber Government business policy ( $M = 2.7186$ ,  $SD = 0.61905$ ) with the lowest mean score was perceived on the overall as least factor that affects cyber business growth. The standard deviations were quite high, indicating the dispersion in a widely-spread distribution. This means that the effects of those above-mentioned factors on cyber business growth are an approximation to a normal distribution. This also indicates that respondents were in favor of cyber business growth.
- ✎ The relationship between cyber legislation and cyber business growth is examined in the above analysis. The result shows that cyber legislation had an insignificant effect on the growth of cyber businesses.
- ✎ The results reveal that government business policy has a positive, and significant effect on Cyber Business growth. It has been found that GBP ( $\beta=0.412$ ,  $t=6.040$ ,  $p<0.001$ ) has the highest influence on Cyber Business growth at ( $p<0.01$ ) level of confidence. This shows

that most cyber actors are dissatisfied with the government business policy, and regulations. In this study government business policies are those things related to licensing registration, work permission, sector certificate of competency, and national strategy. The results imply that the respondents of this study believe, and view GBP as an important factor.

- ✎ The Solution Demand was found to have a positive, and significant effect on Cyber Business growth in the analysis. It has been found that solution demand ( $\beta=0.290$ ,  $t=4.0083$ ,  $p<0.001$ ) has the highest influence or significant impact on Cyber Business growth at ( $p<0.01$ ) level of confidence. The majority of the respondents of the study agreed that solution demand is a very critical factor that challenges cyber business growth., and they manifest that one of the most challenging factors is lack of solution demand. Many studies point out the positive relationship between cyber solution demand and Cyber Business growth
- ✎ The other factor that the analysis is found to give credit is for skilled manpower. Skilled manpower is a challenge for not only Ethiopia, but it is also in the world as well, on the empirical research review we have seen that there will be a need for over 4 million skilled manpower is needed for 2021 in the world (UNCTAD, 2020). This is also a challenge for Ethiopia as well because there will be a competition to migrate cyber literate skilled manpower from Ethiopia. Also, most of the respondent's responses to their open-ended question are the most challenging factor is the migration of skilled manpower. The study shows the cyber skilled manpower, and cyber business growth has a significant relationship, and cyber skilled manpower positively affects cyber business growth.
- ✎ Based on mean and standard deviation The increase in Cyber Firms with ( $M = 3.2932$ ,  $SD = 0.57848$ ), indicate that the increase cyber firms is 3<sup>rd</sup> most dominant factor for business growth. In fact from the respondents of questionnaires, most of the startup cyber firms are challenged by business policy and regulation.
- ✎ Findings from respondents, Most of the respondents recommend that government business policy and regulation, cyber awareness and skilled manpower is a key challenges for the growth of the cyber business.

## 5.2 Conclusion

In this study, it can conclude that those factors mentioned above have a direct impact on business growth. when there is a highly cyber aware society the cyber solution demand is increasing, and when the number of cyber business firms increases the cyber business environment is also improved. Also, the more cyber incident, and attack the more solution demand will be increased so as the cyber business sales increase in sales volume so that it improves the cyber business environment. Also, government cyber business policy is an obstacle so that if we improved this, we can say the number of cyber business firms is improved so that the more the business firms the more competition will be in place this leads the business to grow.

Finally, we can conclude that Solution Demand, Government Business policy Skilled Manpower, and the increasing number of cyber firms have a direct relationship with cyber business growth, and we can say that they can affect cyber business growth.

## 5.3 Recommendation

Based on this study, and findings the following recommendation are made to the government of Ethiopia, Information network security agency, the ministry of innovation, and technology, and ministry of trade, and industry who are responsible for the improvement of the country's cyber environment, and business growth.

- ✎ The business regulation should be reviewed, and must be easy to do business, besides those challenges of starting, and working as a cyber company must be assess, analyze, and fulfill the gap.
- ✎ There is a paradigm shift of the world economy to digital, and virtualization, by considering this government policymaker should review the educational curriculum to consider cyber concerns, which is related to cyber business, and give special attention to it.
- ✎ Security policy, and procedures like cyber-crime policy, should be in place to control cyber theft and any incidents in every organization. Not Only In place but those already developed policies like Critical Mass cybersecurity requirement standard and other policies should be followed regularly, and should be creating awareness on those policies.



- ✎ The government should encourage startup private cyber firms in different mechanisms, like tax exemptions, providing a free working place, and market integration, to improve the growth of the cyber business.
- ✎ For any cyber solutions that would be demanded by the government, the government should place policies that enforce Joint Development to create knowledge transfer as well as technology transfer.
- ✎ In this study, when we analyze the reliability of the measurements of dependent variable i.e cyber business growth, Cronbach's Alpha is resulted with (0.742) this indicates that 74.2% of the dependent variable measurements represent cyber business growth. The rest 25.8 percent are other variables not included in this study. Table 3.3 presents the consistency of measures based on statistics tool

Overall, the majority of the respondents are putting government business policy, and cyber solution demand would be the first two factors that need special attention. One may wonder why this research focuses on cyber-related issues; it is because currently, cybersecurity business is a 6 trillion-dollar issue in the world (Roth, 2020).

IJSER

## References

- Author(s) : Makarand Sinnarkar, S. B. (Mar 2019). *Cyber Security Market*. Pune Nagar Road: allied market research.
- Business Insider . (2020, Feb 2). *cybersecurity-industry-report-investment-case/*. Retrieved from <https://solidbridge.co>: <https://solidbridge.co/cases/cybersecurity-industry-report-investment-case/>
- Cisco. (2020, April wednesday). *what-is-cybersecurity.html*. Retrieved from <https://www.cisco.com/> : <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>
- Dublin. (2019, January 10). *Global Cyber Security Market 2018-2025: Market is Projected to Exceed US\$ 177 Billion*. Retrieved Feb 28, 2020, from Globenewswire: <https://www.globenewswire.com/news-release/2019/01/10/1686006/0/en/Global-Cyber-Security-Market-2018-2025-Market-is-Projected-to-Exceed-US-177-Billion.html>
- EGA. (2020, April 30). <https://ncsi.ega.ee/country/et/?pdfReport=1>. Retrieved April 30, 2020, from <https://ncsi.ega.ee/country/et/>: <https://ncsi.ega.ee/country/et/?pdfReport=1>
- EUROPEAN COURT OF AUDITORS. (March 2019). Challenges to effective EU cybersecurity policy. *Challenges to effective EU cybersecurity policy*, 74.
- FMI. (2019, June 17). *global-cyber-security-market*. (Future Market Insight) Retrieved June 17, 2020, from <https://www.futuremarketinsights.com/reports/global-cyber-security-market>: <https://www.futuremarketinsights.com/reports/global-cyber-security-market>
- Fortune Business Insights. (2019, March 3). *cyber-security-market-101165*. Retrieved from <https://www.fortunebusinessinsights.com/>: <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>
- Fortunebusinessinsights. (2020, Feb 22). *cyber-security-market-101165*. Retrieved February 28, 2020, from [www.fortunebusinessinsights.com](http://www.fortunebusinessinsights.com): <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>
- Herjavec Group. (2020). *The 2020 Official Annual Cybercrime Report*. West Hollywood, California: Herjavec Group.
- INSA. (2014, January 2nd). A proclamation to Reestablish The Information Network Security Agency. *Proclamation No. 808/2013*. Addis Ababa, Ethiopia: Birhanina selam Printing press.
- itgovernance. (2020, April 27). *what-is-cybersecurity*. Retrieved from <https://www.itgovernance.co.uk/>: <https://www.itgovernance.co.uk/what-is-cybersecurity>
- Markets and Markets. (2018, sep). *Cyber Security Market*. Cyber Security. Retrieved from <https://www.marketsandmarkets.com>: <https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html>

- MarketWatch. (2020, June 2). *cyber security market size and share forecast to 2024/Global Industry Analysis by dynamics Trends, Company overview, growth factors*. Retrieved from [www.marketwatch.com](http://www.marketwatch.com).
- Micro Market Monitor. (2015, Nov 3). *middle-east-and-africa-cyber-security-9122775574.html*. Retrieved from <http://www.micromarketmonitor.com>:  
<http://www.micromarketmonitor.com/market/middle-east-and-africa-cyber-security-9122775574.html>
- Micro Market Monitor. (2017). *North America Cyber Security Market Research Report*. US/CAN: micro market monitor. Retrieved 2020, from <http://www.micromarketmonitor.com/market/north-america-cyber-security-6364811086.html>
- MicroMarketMonitor. (2015, Nov 15). *asia-pacific-cyber-security-9409640255.html*. Retrieved from <http://www.micromarketmonitor.com>: <http://www.micromarketmonitor.com/market/asia-pacific-cyber-security-9409640255.html>
- micromarketmonitor. (2015, Nov 2). *europa-cyber-security-4129808188.html*. Retrieved from [www.micromarketmonitor.com](http://www.micromarketmonitor.com): <http://www.micromarketmonitor.com/market/europe-cyber-security-4129808188.html>
- Reba, M. B. (2005, June). STATE OF CYBER SECURITY IN ETHIOPIA. Addis ababa.
- Research, O. (2020, January 10). *marketwatch*. Retrieved Feb 28, 2020, from [marketwatch](https://www.marketwatch.com/press-release/latin-america-cyber-security-market-2020-regional-demand-current-trends-applications-key-players-analysis-and-forecast-to-2024-2020-01-10):  
<https://www.marketwatch.com/press-release/latin-america-cyber-security-market-2020-regional-demand-current-trends-applications-key-players-analysis-and-forecast-to-2024-2020-01-10>
- Roth, J. A. (2020, June 15). [https://www.iiba.org/iiba-analyst-catalyst-blogs/\\$6-trillion-is-expected-to-be-spent-globally-on-cybersecurity-by-2021/](https://www.iiba.org/iiba-analyst-catalyst-blogs/$6-trillion-is-expected-to-be-spent-globally-on-cybersecurity-by-2021/). Retrieved from [www.iiba.org/iiba-analyst-catalyst-blogs/](http://www.iiba.org/iiba-analyst-catalyst-blogs/): [https://www.iiba.org/iiba-analyst-catalyst-blogs/\\$6-trillion-is-expected-to-be-spent-globally-on-cybersecurity-by-2021/](https://www.iiba.org/iiba-analyst-catalyst-blogs/$6-trillion-is-expected-to-be-spent-globally-on-cybersecurity-by-2021/)
- solidbridge. (2020, April 22). *cybersecurity-industry-report-investment-case/*. Retrieved from <https://solidbridge.co>: <https://solidbridge.co/cases/cybersecurity-industry-report-investment-case/>
- UNCTAD. (2020, Feb 04). *eCom-Cybercrime-Laws.aspx*. (UNODC) Retrieved April 30, 2020, from <https://unctad.org>: [https://unctad.org/en/Pages/DTL/STI\\_and ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx](https://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx)
- Whitehouse. (2020, April 2). *ap\_24\_cyber\_security-fy2020.pdf*. Retrieved from <https://www.whitehouse.gov>: [https://www.whitehouse.gov/wp-content/uploads/2019/03/ap\\_24\\_cyber\\_security-fy2020.pdf](https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf)
- Ahmed, Nadeem & Kulsum, Umme & Azad, Md & Momtaz, A & Haque, M. & Rahman, Shahriar. (2017). Cybersecurity awareness survey: An analysis from Bang bladesh perspective. 788-791. 10.1109/R10-HTC.2017.8289074.

## Appendix A

### Survey Questionnaire

**Dear Respondent**

#### The objective of the questionnaire

This questionnaire is used for the educational purposes the purpose of the research conducted for the improvement of the cyber business environment so that assessment on key stakeholders, employees, and business owners are considered to be vital, and critical.

#### Part 1: Demographic Data

1.	Gender/SEX		Male	Female	
2.	Age Group	25 or Below	26-35	36-50	Above 50
3.	Education Status	Diploma or Below	Degree	Masters	PhD
4.	Work Experience	1 or Bellow	2-5	5-10	Above 10
5.	Occupation	Owner	Manager	Expert/Employee	

#### Part 2: Cyber Business Growth Factors

##### Definition

**Cyber** – any computer, software, mobile, network, telecom line, electromagnetic, and information communication devices.

**Cyber business** – any business which is related to software, security, computer, network, and other cyber-related activities which includes import-export of information communication devices.

**Cyber Attack/Crime** – any incident that harms your computer, and information asset, it may include your computer, your mobile, and tablets.

##### Instruction

 **Just Tick your choice**

**Select only one choice**  
**If you have no idea about the question select Neutral**

No	Question	Scale				
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
<b>Cybersecurity Awareness</b>						
1.	you have a security policy and guidelines on your organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2.	As an organization, you will get planned security awareness training?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.	cybersecurity is considered as Core component of the organization?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4.	You have awareness of key organization information assets.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5.	You have enough knowledge on how to protect your computer, mobile, and tablets from attack.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6.	You have enough knowledge about security solutions that are provided by cybersecurity firms.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Cyber Legislation</b>						
7.	There is cyber policy, and Legislation Nationally to help guide government or private firms regarding cybersecurity solutions.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8.	There is Cybercrime Law and regulation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9.	There is a Cybersecurity Requirement standard.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10.	Nationally there is cybersecurity Stated Standard Framework Like NIST.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The demand for cybersecurity solutions							
11.	There is a continuous demand for cyber-related solutions on your organization	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
12.	Cyber firms provide solutions as per expected or demanded quality standard	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
13.	The demand of cyber solution increase in national level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Skilled Manpower							
14.	There are experts Turnover on your organization who work on cyber-related functions.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
15.	You have certified professional cyber experts in your organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
16.	It is easy to get and recruit skilled manpower regarding information security.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
17.	Government education policy helps to easily available information security skilled manpower.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Cybersecurity Firms							
18.	Cybersecurity firms are increasing in number	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
19.	most new cyber firms early exist/terminate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
20.	Most of the firms are standard and provide the expected solutions or user needs.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Government Business policy, and regulation:							
21.	There is Support from Government through policy, and regulation to help improve the cyber environment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

22.	Appropriate international and local business policy is in place to start a cyber business.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
23.	The government provides Incentive factor-like Tax exemption, providing a working place, and other facilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
24.	It is easy to start and exit the cyber business.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Cybersecurity incidents/Cybercrime</b>						
25.	you are facing continuous personal cyber-attack or incidents on your mobile, and personal devices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
26.	Frequently cyber-attack happened on organization information assets.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
27.	You have enough information about incidents and cyber-attack on your organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Cyber business Growth</b>						
28.	Employment in cybersecurity business increasing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
29.	The profitability of cyber firms in Ethiopia is increasing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
30.	There is job satisfaction in employees who work on cyber firms in Ethiopia.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
31.	Sales volume of cyber product in cyber firms are increasing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>cyber business Growth</b>						
<p>☒ What do you think about the challenges of new cyber business firms from growth in Ethiopia?</p> <ol style="list-style-type: none"> <li>1.</li> <li>2.</li> <li>3.</li> </ol> <p>☒ What do you suggest that must be improved to improve productivity, and growth of cyber business firms?</p>						

Table Error! No text of specified style in document.1 Questionnaires

32. What do you think about the challenges of new cyber business firms that are being an obstacle to the growth in Ethiopia?

- ✗ The main reason is the infrastructure, and the skilled professionals will travel to foreign countries to get a good job with a high salary. we can say we have no skilled employees.
- ✗ Latent industry demand.
- ✗ Incentive, international competitions, and confidence in local products, and services
- ✗ Policy, and public awareness of cybersecurity
- ✗ Lack of awareness.
- ✗ Clients' awareness of the importance of investing to purchase such services, and firms' infrastructure able to provide service.
- ✗ 1.basic infrastructure is not available before we talk about cyber issue, and even basic concept about cybersecurity is not introduced to the society
- ✗ It's something new, and finding policy/guidance will be a challenge.
- ✗ Policy, skilled manpower
- ✗ minimal-Value that organizations are giving for cybersecurity
- ✗ minimal-Value that organizations are giving for cybersecurity
- ✗ unavailability of cyber legislations, unavailability of skilled manpower, and total unawareness, and low attention to the area by the nation.
- ✗ Connectivity, internet payment, and lack of clear cybersecurity policy
- ✗ first the government has driven rule, and regulation timely, and also governmental, and

33. What do you suggest that must be improved to improve the productivity, and growth of cyber business firms?

- ✗ Create awareness of the importance of cyber business firms, and how they can Simplify our day to day activity. Facilitate a good infrastructure for the business.
- ✗ Cybersecurity policy, strategy, standard, guideline
- ✗ Legal support
- ✗ Government commitment towards cybersecurity firm concerning the legal framework, and incentive mechanisms
- ✗ Policy, and public awareness of cyber business firms

Specialized Educations, more Conferences, and researches, and strong infrastructures on Cyber-Security industry

- ✗ 1.basic concept awareness and the sector must be outsourced to a private company, and the government must give incentive who works on this sector
- ✗ First, the firms need to create awareness to companies or organizations on its importance and create demand.
- ✗ Strong check, and evaluation to check the correct implementation in organizations.
- ✗ Awareness programs should be prepared to give information on the values of cybersecurity
- ✗ First, and for most planned awareness pieces of training should be given to the public, and global cyber Legislation should be accepted fully as a nation, and The nation has to give enough attention to the area, etc.

Cybersecurity policy, and skilled manpower training.

The Government should incorporate Cybersecurity course in higher education curriculum



other business sectors top-level management should aware the impact of cyber-warfare

✗ lack of Awareness @ stockholders

There should be regulations, and directives on the standard nationwide., and also give pieces of training especially in educational institutions.

✗ Lack of awareness of cybersecurity services, business leaders in Ethiopia like to invest their money on something that could be seen or touched like data centers but fails to understand how to protect it so creating awareness is a key.

First, and for most security awareness training needed to be conducted. Business leaders need to understand the threat landscape, and how it affects their organization. Cybersecurity consulting companies also need to paint the right picture to those business leaders. In Ethiopia, we probably have been breached several times but companies don't know it or care about it. Especially these days since people connected to the Internet is increasing there will also be an increase in cyber attacks but companies need to start in implementing solution before attacks become common.

✗ The risk is internal (human) than external cyber attacks as most of our systems are not exposed to the internet.

An open, and internet-based competitive business encouragement that makes cybersecurity a critical necessity.

✗ lack of skill capacity, and government policy.

the first thing is to create cybersecurity awareness in all CEO, Director, and Technical experts

✗ Other people's lack of knowledge about cybersecurity

✗ Lack of enough understanding of companies about the cyber systems.

Creating awareness about cybersecurity system

✗ Awareness creation, shortage of cooperation with organizations, and Cyber business

the government's willingness to cooperate on automating their systems.

Creating awareness in the organizations.

✗ Awareness is the most important, and it needs big investment in the sector because of this no one interested in this challenge the government must support this sector by creating awareness, and possible action to promote this filed in its Education plan.

They have to work with the government by creating awareness about threats and damages it create to the business.

✗ 1. Government authority 2. Technology adaptability 3. Understanding the target market

1. Other than providing product solution to the customer, also develop a cyber-security training program to enhance productivity.

<p>✗ Because there is little awareness about the importance of cyber implementation</p>	<p>To increase the awareness level of individuals</p>
<p>✗ government policy structure</p>	
<p>✗ Security Awareness</p>	<p>support from top management</p>
	<p>universities and research institutes should have participated in cybersecurity research</p>
	<p>there should be a clear cybersecurity policy and standards that should</p>
<p>✗ lack of clear establishment standards, and policies, and it is considered as single body responsibility</p>	<p>be known by the users</p>
	<p>efficient, and effective cybersecurity manpower has to be produced by universities</p>
	<p>Cybersecurity framework must be prepared by the government</p>
<p>✗ I don't think there is a national policy or any enforcement</p>	<p>Cybersecurity regulations and standards must be enforced.</p>
	<p>Create awareness on what it is, why it is required for a business firm,</p>
<p>✗ Business firms don't take it as a requirement, so the need is low.</p>	<p>revise government policy/policies, encourage those firms who work on the issue using tax exemption or other methods.</p>
<p>✗ some multinationals like tax-exempt, loan, and provide human power</p>	<p>✗ Government need to budget and educate</p>
	<p>✗ INSA is a kind of a Monopoly regarding Cybersecurity ( for example it is involved with all the banks ). The agency has to give way gradually to private companies.</p>
<p>✗ I think Brain Drain is the major issue.</p>	<p>✗ Awareness creation on the multidimensional negative impact of cyber-attacks which could cripple the much indispensable cyberinfrastructure. Companies should invest in their infrastructure, and human power, do more security hardening tasks on the available/deployed infrastructure with the technology at their disposal. Government should do more in facilitating the production of skilled security engineers, and penetration testers. The government should intensify its a role in creating a National Cybersecurity policy framework, enforce GO, and NGOs to adopt, and strictly apply Cybersecurity frameworks so they set up their Policy, directive, and guideline by combining National, international, and industry standard, and best practices.</p>
<p>✗ Lack of awareness of the mission-critical importance of Cybersecurity when it comes to organization, enterprises, and employees which results in a poor investment of arming their infrastructure with a security solution.end-users, and lack of adequate expertise when it comes to Security Engineers. Lack of a much-needed company level cyber policy, and directive in local organizations. These all resulted in low cyber investment.</p>	<p>I was planning on studying my graduate degree in Cybersecurity after I learned that AAiT was offering it, to find</p>

✎ Lack of awareness of the mission-critical importance of Cybersecurity when it comes to organization, enterprises, and employees which results in a poor investment of arming their infrastructure with a security solution.end-users, and lack of adequate expertise when it comes to Security Engineers. Lack of a much-needed company level cyber policy, and directive in local organizations. These all resulted in low cyber investment.

✎ Awareness

✎ Awareness!

✎ Company's Acceptance, and understanding

out later that this program was being provided to folks who are only from INSA. This kind of practice which monopolizes the spread of the much-needed education, and research, stifles the growth of the Cybersecurity industry as a nation by denying outsiders from acquiring the skill.

✎ Awareness creation on the multidimensional negative impact of cyber-attacks which could cripple the much indispensable cyberinfrastructure. Companies should invest in their infrastructure, and human power, do more security hardening tasks on the available/deployed infrastructure with the technology at their disposal. Government should do more in facilitating the production of skilled security engineers, and penetration testers. The government should intensify its a role in creating a National Cybersecurity policy framework, enforce GO, and NGOs to adopt, and strictly apply Cybersecurity frameworks so they set up their Policy, directive, and guideline by combining National, international, and industry standard, and best practices.

I was planning on studying my graduate degree in Cybersecurity after I learned that AAiT was offering it, to find out later that this program was being provided to folks who are only from INSA. This kind of practice which monopolizes the spread of the much-needed education, and research, stifles the growth of the Cybersecurity industry as a nation by denying outsiders from acquiring the skill.

R&D

✎ The government must understand the impact of Cybersecurity by consulting outstanding Ethiopian Professionals who work on the professional half of their lives. undertake research and development of the area. not for political consumption but for ICT4D

✎ Create awareness for the concerned organizations, and the government should open the business for private owned companies.

✎ Proper, and timely training

- ✗ Awareness of organizations, and the attention is given for the field
- ✗ lack of updates, and skilled manpower, Organisational awareness on cyber Security
- ✗ Lack of Cybersecurity awareness in organizations & Corporate Managers, Lack of encouraging government policy working in Cyber-security, and lack of government higher education in Cybersecurity are some of the challenges/obstacles in the Cyber Business in Ethiopia.
- ✗ Some of the challenges and problems include a high level of unemployment, high poverty incidence, lack of managerial skills, and low industrialization capacity, lack of finance, inconsistent government policies, and inadequate infrastructure, and insecurity of the business climate among others.
- ✗ It's challenging but needs some policy and procedural help from the government side.
- ✗ It's challenging but needs some policy and procedural help from the government side.
- ✗ Market, and motivation
- ✗ Awareness level of the public
- ✗ Professionals, lack of policies, regulations, Awareness
- ✗ In Ethiopia, It is So Seen that more traditional Approach challenge for the new cyber Business Firm not to growth
- ✗ increase skilled manpower, incentives from the government
- ✗ Cybersecurity Awareness for top Management Officials, & Government Policy Makers
- ✗ increasing Cybersecurity awareness training in Organizations, and Corporations, encouraging Cybersecurity firms by through incentives, and favorable working environments & policies
- ✗ 1. Change Your Passwords.
- ✗ 2. Use a Password Manager.
- ✗ 3. Delete Any Unused Accounts.
- ✗ 4. Enable Two-Factor Authentication.
- ✗ 5. Keep Your Software Up to Date.
- ✗ creating awareness to the nation, and giving important training on the issue
- ✗ Governmental help and professional training for IT personnel are needed.
- ✗ Governmental help and professional training for IT personnel are needed.
- ✗ Financing, incentives provision, and competitiveness arrangements are expected from INSA
- ✗ Creating awareness on the demand side, and enabling environment on the supply side by concerned entities.
- ✗ Policies, and regulations
- ✗ Most organizations adopt the Manuel and routing business processes than preferring life easy processes so that makes the cyber productivity backward ever time. So that I suggest, the more you approach to use the technologies the more you become vulnerable So the organization should focus on those Cyber Policy, and all businesses regard to cyber early focus, and should work in day to day activity.

<input type="checkbox"/> Adoption	<input type="checkbox"/> Policy
<input type="checkbox"/> Poor governmental business policy, and regulation	<input type="checkbox"/> Developing good governance policy, and providing cybersecurity awareness training to the societies.
<input type="checkbox"/> Lack of cyber-security professionals Ethiopia	<input type="checkbox"/> To create good knowledge on the need of cybersecurity., and practically implementing cyber
<input type="checkbox"/> Awareness problems	<input type="checkbox"/> User awareness of different types of attacks
<input type="checkbox"/> the license provision for security firm is the same as the other ICT business licensing, and there is no background checking, and government incentives to manipulate the cyberspace	<input type="checkbox"/> provide incentives start license provision which is not the same as the other technology support, and certify training centers support startups, and firms financially
<input type="checkbox"/> Investment, and skillsets	<input type="checkbox"/> Affordability
<input type="checkbox"/> The legal process to start a business	<input type="checkbox"/> The government should support cyber firms
<input type="checkbox"/> The government limitation, and other business laws.	<input type="checkbox"/> We need a clear to understand law fir every cyber business. We also need support, especially for startup online businesses.
<input type="checkbox"/> Government organizations like insa, and telecom	<input type="checkbox"/> Government policy towards cybersecurity is key
<input type="checkbox"/> Low economy growth, and lack of skilled manpower	<input type="checkbox"/> Skilled manpower, and support from the Government
<input type="checkbox"/> Organization awareness about the need for cybersecurity in the company	<input type="checkbox"/> Creating awareness , decreasing cybersecurity cost
<input type="checkbox"/> Lack of national policy, and regulatory framework.	<input type="checkbox"/> Provision of the regulatory framework, and expansion of the Internet.
<input type="checkbox"/> Most companies are not aware of the need for cybersecurity,...and they don't see a need to invest in it	<input type="checkbox"/> right education, trained people, awareness, and focus on cybersecurity threats,
<input type="checkbox"/> No enough awareness, and benefit for cyber business firms	<input type="checkbox"/> improve the capacity of Human resources in Cybersecurity
<input type="checkbox"/> Lack of national policy, and regulatory framework.	<input type="checkbox"/> Give strong awareness about cybersecurity to companies, Train IT professionals in the cybersecurity area, companies should implement the latest technologies and methods that other countries use.
<input type="checkbox"/> n/a	<input type="checkbox"/> Provision of the regulatory framework, and expansion of the Internet.
	<input type="checkbox"/> First of there need to be demand from organizations

✕ Government policy

✕ The public is not aware of their functions, and their main challenge is in increasing awareness, and knowledge of preventing cyber attacks.

✕ The gap mentioned above as there are no such policies, and regulations which force institutions to follow, and comply, the demand for security solutions, and services are being assumed as luxury requirement except few industries like the financial sector, and the telco

✕ - Invest in the employee's knowledge by giving them training  
- Let them experience abroad, and another growing country on cybersecurity  
- Work with the government on the policy

✕ There should be funding from the government.

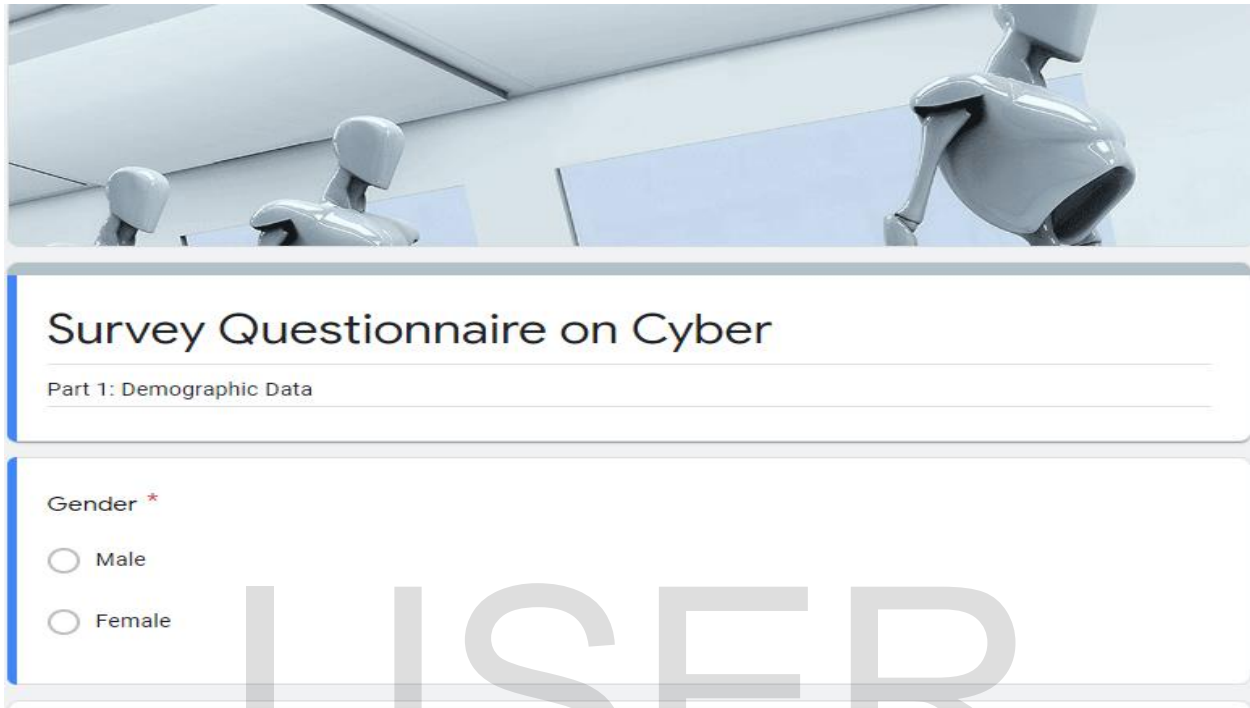
✕ - Government policy must change to participate in private actors in the cyber business.  
-Gov't Should Appreciate small business firm work on the cyber business.  
- education is a must to empower youth on cybersecurity business so the government and private institutions must include cyber education on their curriculum.

✕ - Government policy must change to participate in private actors in the cyber business.  
-Gov't Should Appreciate small business firm work on the cyber business.  
- education is a must to empower youth on cybersecurity business so the government and private institutions must include cyber education on their curriculum.

✕ Strong support from the government is needed for the business, and the govt itself should have a well, and in detail defined cybersecurity policies, regulations, processes, and frameworks for all gov, and non-gov businesses, and institutions nationwide.

## Appendix B

Screen Shoot of online Questionnaires



Survey Questionnaire on Cyber

Part 1: Demographic Data

Gender \*

Male

Female

IJSER

### Cyber Legislation

9. There is Cyber security Requirement standard which guides any security specification implementation of any information systems, software and infrastructure. \*

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

7. There is cyber policy and Legislation Nationally to help guide government or private firms regarding cyber security solutions. \*

- Strongly Agree

### Response View of Survey

Survey Questionnaire On Cyber



Send

Questions Responses

responses



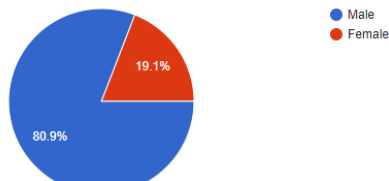
Accepting responses

Summary

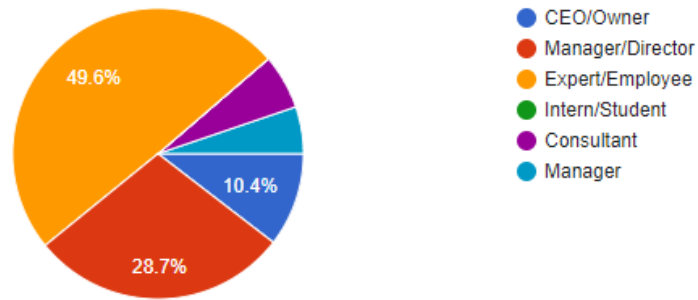
Question

Individual

Gender



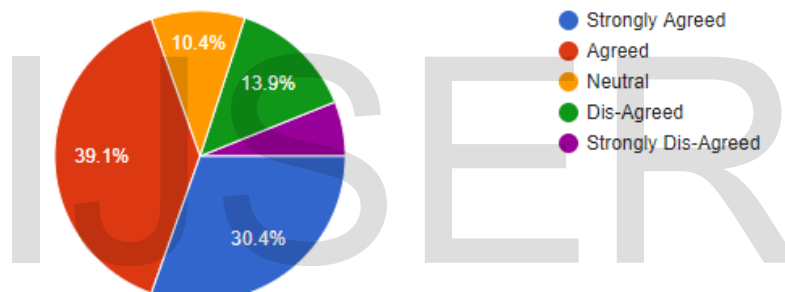




### Cyber Security Awareness

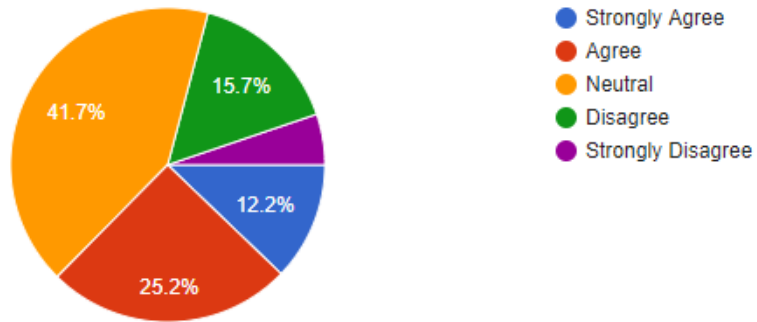
1. you have a security policy and guideline on your organization.

115 responses



14. There is experts Turnover on your organization who work on cyber related functions.

👤 responses



15. You have certified professional cyber experts on your organization.

👤 responses

