# Measuring Cybersecurity Awareness in Somalian Organizations

**BY**

**HAMZA AHMED ABDLAAHE**

**ID:0242310005343004**

This Report in Partial Fulfilment of The Requirements for The Degree of Masters of Science in Software Engineering

Supervised By

**Dr. A. K. M. Masum**

Professor, Department of Software Engineering

Daffodil International University


**DAFFODIL INTERNATIONAL UNIVERSITY**

**DHAKA, BANGLADESH**

**JANUARY 2024**

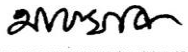
# APPROVAL

This thesis/project/internship titled on "**Measuring Cybersecurity Awareness in Somalian Organizations**", submitted by Hamza Ahmed, ID: 0242310005343004 to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Masters of Science in Software Engineering and approval as to its style and contents.

**BOARD OF EXAMINERS**

---------- Chairman

Dr. Abdul Kadar Muhammad Masum
Professor
Department of Software Engineering
Daffodil International University



---------- Internal Examiner 1

Afsana Begum
Assistant Professor
Department of Software Engineering
Daffodil International University

---------- Internal Examiner 2

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Daffodil International University

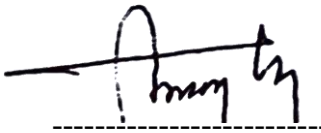
---------- External Examiner

Md. Tanvir Qadeer
Senior Software Engineer,
Technology Team,
a2i Program

# DECLARATION

I announce hereby that I am rendering this study document under **Dr. A. K. M. Masum, Professor**, Department of Software Engineering Daffodil International University. I, therefore, state that this work or any portion of it was not proposed here therefore for Bachelor's degree or any graduation.

## Certified by:



---

**Dr. A. K. M. Masum,**

Professor

Department of Software Engineering

Daffodil International University

## Submitted by:

---

**Hamza Ahmed**
ID: 0242310005343004
Department of Software Engineering
Daffodil International University

# ACKNOWLEDGEMENT

First and foremost, I sincerely appreciate and am grateful to the Almighty God, without his divine blessing it would be impossible for me to successfully finish my final year thesis.

I would like to sincerely thank Dr. Engr. A. K. M. Masum, my supervisor and a professor of Daffodil International University's Software Engineering department. His wise counsel, helpful direction, and unwavering support have all been crucial to the accomplishment of this thesis. Throughout this journey, his knowledge and commitment have been invaluable to my academic and personal development.

Our coordinator, Ms. Afsana Begum, has my sincere gratitude for her unwavering support, prompt help, and availability to answer any questions or issues I may have. Her commitment and organizational abilities made the process go well, and for that I am really appreciative.

I would especially want to express my gratitude to Dr. Imran Mahmud, the associate professor and head of the department of software engineering. His inspirational guidance, encouragement, and support have made a positive impact on research and academic achievement. His dedication to the department and the academic achievement of the students is really motivating.

I would want to express my thanks to every member of the Software Engineering department teacher, staff, and student who has helped and encouraged me with my study. This trip has been enjoyable because of their contributions and friendship.

Finally, I want to express my gratitude to my friends and family for their constant understanding, tolerance, and support during this process. Their support and affection have given me courage and strength.

Thank you all for your significant contributions to the completion of this thesis.

# ABSTRACT

The rise in Cybercrime is a result of technological breakthroughs and inventions, which has led many cyber specialists and researchers to focus more on Cybersecurity. Software, hardware, and other computer components are all protected by Cybersecurity. Cybercrimes may be committed as a result of cyber attackers gaining access to communication controls and remote-control weapons. Cybersecurity should therefore not be taken lightly; rather, careful thought should go into its implementation. In this research, I employed a quantitative approach to gather quantifiable data from employees in different Somalian organizations using Google Form to distribute meticulously thought-out survey questionnaire to investigate how employees in different Somalian companies perceive and feel about Cybersecurity. The techniques utilized to analyze the data that was gathered include Pearson correlation, variance analysis, and independent t-test. The findings indicated that the alternate hypothesis, which was accepted, is connected to the beta value forage applied to the attitude toward Cybercrime and Cybersecurity in business. This suggests a positive significance and, consequently, suggests that the age of the employees had a significant influence on the attitude toward Cybercrime and Cybersecurity in business. "Gender," which is linked to the null hypothesis being accepted, did not demonstrate any relevance, suggesting that there was no gender-related positive attitude on Cybersecurity in company. The phrases "position at work" and "experience" indicate that the significance was sufficiently positive to lead to the employees' general good attitude toward their varied office jobs and experiences. Therefore, our research can help Somalian companies strengthen their cyber defenses and guard against online fraud when conducting business.

# TABLE OF CONTENT

# List of Figures

# List of Tables

## Lis of abbreviations

| | |
|---|---|
| **ANOVA:** | Analysis of Variance |
| **ATC-IB:** | Attitudes towards Cybersecurity in business |
| **BBC:** | British Broadcasting Corporation |
| **CERT:** | Computer Emergency Response Team |
| **CIA** | Confidentiality, Integrity, and Availability |
| **EVC** | Electronic Voucher Card |
| **FIRST** | Forum of Incident Response and Security Teams |
| **HTML:** | Hypertext Markup Language |
| **ICT:** | Information and Communication Technology |
| **IP:** | Internet Protocol |
| **ISPC:** | information security policy compliance |
| **ISAP:** | Information Security Attitude Program |
| **NCA** | National Communications Agency |
| **PMT** | Protection Motivation Theory |
| **SPSS:** | Statistical Packages for Social Sciences |

# Chapter 1
# Introduction

The increasing relevance of Cybersecurity in the digital age driven by increased cyber activity and technical advancements is covered in this chapter's introduction to the study. It presents the problem description and draws attention to the Cybersecurity infrastructure vulnerabilities in Somalia. The goal of the study is to assess Cybersecurity knowledge among workers in different Somalian companies. Additionally, it describes the research's limits and significance.

## 1.1 Overview on Cybersecurity

Researchers and Cybersecurity specialists are paying close attention to the surge in Cybercrime that has resulted from technological developments and an increase in cyber activities. Because it protects computer systems' hardware, software, and other informational components, Cybersecurity is essential in the digital sphere [1]. Because Cybersecurity is so effective at thwarting online dangers like malware, fraud, and other Cybercrimes, its importance has grown. Studies conducted over the years have shown that stricter laws are needed to support Cybersecurity measures [2].

Internet banking has been a major factor in internet fraud, which increased 64% to over $174.4 million in 2015, [3]. This increase was mostly caused by flaws in online protection systems. Malware attacks have been common in the cyber world, especially in online banking. Wazid [4] have recently discussed how mobile banking has evolved and how vulnerable it is to malware threats. Though some malware remains undetectable by these techniques, the creation of numerous software tools for malware detection, protection against, and removal has been advantageous [5].

With the advancement of the internet, hackers now have more power than ever before. They can remotely take over power supplies, communication networks, and even weapons, which could result in acts of terrorism or genocide. As a result, Cybersecurity is serious business and demands large investments in safeguards [6]. For example, a cyberattack in late December 2015 resulted in a power outage in Ukraine, posing a threat to national security and causing significant economic damages. Malware was used to obtain data from different systems. Governments need to implement Cybersecurity laws strictly because hackers can use a country's domain to conduct

attacks that have the potential to turn into global conflicts or wars. Cyber dangers cannot be completely eliminated, but their effects can be lessened by using tools like firewalls, which can identify potentially dangerous data. Firewalls can be exploited by cyber attackers due to their weaknesses, which include the inability to recognize spoof messages [7]. A lot of software and apps are weak, especially when they're installed on devices without strong antivirus software. Nowadays, scams are the most prevalent type of Cybercrime, with many people and businesses falling for con games on a daily basis. Because scams are more difficult to neutralize than other malware attacks, they present a challenge for Cybersecurity professionals. Furthermore, users occasionally turn off security protections, which makes an application more vulnerable [8].

Because of the interconnectedness of the global internet community, underdeveloped countries are not immune to cyberattacks, even if they are more common in developed nations. Organizations, especially those in Somalia, need to realize how important Cybersecurity is since weak defenses leave them vulnerable to attacks from scammers and rivals. Reducing Cybercrime and improving internet safety procedures can be accomplished by raising awareness of Cybersecurity perceptions within Somali enterprises and encouraging a proactive approach.

### 1.2 Problem Statement

Globally, digital technologies are developing at a rapid pace, but Somalia's Cybersecurity infrastructure is still in its infancy, and both the commercial and nonprofit sectors have serious vulnerabilities. As a company's first line of protection, employees are essential to preserving Cybersecurity. On the other hand, nothing is known about how Somali firms' personnel views the Cybersecurity measures that are currently in place.

This study fills a major knowledge gap about the efficacy of current Cybersecurity policies from the perspective of information technology-dependent registered enterprises' employees. The risk of cyber threats is increased in the absence of a national Cybersecurity strategy, a legally recognized Computer Emergency Response Team (CERT), and national Cybercrime regulations. This could result in financial losses, compromised personal and organizational data, and a decline in public confidence in digital systems.

The issue is made worse by the diverse structure of Somalia's employee base, which is comprised of small and large businesses with differing degrees of Cybersecurity knowledge and IT implementation. The goal of the study is to shed light on employee attitudes, perspectives, and knowledge gaps about Cybersecurity in order to help build focused initiatives that will strengthen Somali firms' digital defenses.

### 1.3 Research Objective

The purpose of this study is to critically evaluate Cybersecurity awareness in Somalia, particularly in the workforce. It seeks to understand how employees across a range of businesses perceive the Cybersecurity measures in place. The study aims to determine the primary barriers and gaps in knowledge in Cybersecurity protocols, as well as to assess the effectiveness of current countermeasures against cyberthreats. The study aims to provide insights that could direct the development of more comprehensive Cybersecurity policies and training curricula that are particular to Somalia's evolving digital environment through an investigation of the workforce's views and knowledge of Cybersecurity. The study's primary objectives are to:

- To assess the efficiency of Somalia organizations' cyber-defenses
- To look into the proportion of cyberattacks on Somalia organizations
- To find out how Somalian employees view and feel about Cybersecurity.

### 1.4 Significance of Study

Further research on how to strengthen Cybersecurity is urgently needed given the threat that cybercriminals pose to businesses and their ability to control global resources and power. Nonetheless, many nations, like Somalia, have a poor attitude and view of Cybersecurity. As a result, Somalia organizations can strengthen their cyber defenses and fend off infestations and cyberattacks by consulting previous studies' literature and quantitative study on Cybersecurity in Somalian enterprises.

### 1.5 Limitations of the Study

This report offers a thorough examination of the Cybersecurity landscape as it exists today, including the most common cyberthreats and organizational perspectives of Cybersecurity in Somalia. It provides insightful information about how the workforce views cyberthreats and the protective measures put in place, as well as their awareness

of them. To have a comprehensive grasp of Cybersecurity in Somalia, one must take into account several aspects that the report does not include. The report describes the types of cyberthreats and Cybersecurity levels, but it doesn't go into detail on the specific actions that might be made to enhance Cybersecurity in Somali businesses.

The extent to which Somali institutions are conducting research on Cybercrime is also not examined in the study. Academic research can be extremely important in understanding and combating Cybercrime, therefore this is a serious omission.

# Chapter 2
# LITERATURE REVIEW

This literature review offers a thorough summary of the state of Cybersecurity and Cybercrime research at right now. It discusses the definition, characteristics, and extent of Cybercrime as well as the influence of technology advancement on criminal activity and pertinent theoretical frameworks. It also looks at Cybersecurity procedures in Somalia and the difficulties organizations have in thwarting cyberattacks.

## 2.1 Cybercrime

The term "Cybercrime" refers to the new types of criminal activity made possible by internet. Since this crime is always growing, there is really less effectiveness in using practical steps to combat it. Therefore, new technical approaches are required to handle this developing issue. Understanding criminals' motivations is essential for devising and implementing effective management strategies, but it's equally important to comprehend their victims. Specifically, one must identify the computer system users who become targets of these criminals. This phrase has been given several definitions with varying levels of specificity.

It is necessary to understand how information and communication technology has affected our environment in order to define Cybercrime correctly [9]. Because of the unique features of internet, cybercriminals now have access to unusual chances. According to Jahankhani [9] , these qualities have been dubbed "transformative keys." Among these are:

1. Globalization presents cybercriminals with new opportunities to circumvent conventional constraints.
2. Dispersed networks: those provide new avenues to abuse
3. Synopticism and Panopticism: they enable victims to be remotely monitored
4. Data traces: enable cybercriminals to carry out impersonation

There are three primary degrees of the internet's impact on offender opportunity, according to Wall [10]. Above all, the emergence of cyberspace has made traditional

thefts like fraud, stalking, and chipping more common. These were always common in real life, but the internet has made them more so. Conventional criminals use the internet not only to connect with one another but also to do sophisticated crimes like money laundering and fraud with less risk and more accuracy. Furthermore, the internet has created new opportunities for traditional crimes including hacking, virus distribution, widespread fraud, online pornography, and inflammatory speech. Hacking is the most well-documented type of Cybercrime against it, according to the CIA. However, recent advances have brought forth the practice of "parasitic computing," in which criminals use several remote computers to do tasks such as archiving illegal data, such as stolen software and pornographic photos.

Because cyberspace is so vast, it has opened the door to new criminal activities like spamming, service rejection, property piracy, as well as fraudulent e-marketing. Regarding the psychology of a criminal, there are roughly four primary types of crime. These can be categorized into one of the following four groups:

- Those concerning integrity, such as detrimental infringement
- Those concerning computer use, such as dishonesty and possession by theft
- Those concerning information, such as pornography
- Content-related, such as violence

Jahankhani [9] state that these offenses might be classified as mild, medium, or extremely harmful. For example, chipping is regarded as somewhat destructive in the integrity class, while information warfare and service rejection are deemed to be the most injurious. Much has been said recently on the Table regarding the characteristics of Cybercrime and how to control it. The size, nature, and control of Cybercrime are hotly contested issues [11]. The fight against cyber criminology has been extensively chronicled, and it is always evolving, particularly with the introduction of more advanced computer technology. Absence of a distinct border in its definition presents a significant challenge because it makes it more difficult to specify potential remedies and countermeasures, particularly given the rapidly increasing volume of Cybercrime and its impact on businesses. Cybercrime increased by 60% between 2012 and 2013, According to a remark, the Commissioner of the Metropolitan Police, Sir Bernard Howe, claimed. Moreover, in the same fiscal year, Cybercrime cost the British

economy a staggering 81 billion pounds. This increase is caused by the fact that, in contrast to classic arm robbers, cybercriminology offers enormous money rewards with very little chance of legal repercussions [12].

Cybercrime is committed online, regardless of location, in contrast to traditional crime, which is carried out in a specific area. Thus, international action is required to address this situation. To address the obvious issues that prevent Cybercrime from being managed effectively, this answer is required. A few of these issues relate to technology, the makeup of the nation, and the characteristics of Cybercrime. Historically, the perception of crime has always been confined to a certain social, material, as well as cultural context. This precise description has made it possible to define crime and establish policies for dealing with it. However, as the context of Cybercrime is not limited to any one specific geographic area, culture, or social class, this is not a readily applicable theory. For example, rape and child abuse are examples of traditional crimes that can be classified according to the offender's social standing, place of residence rural vs. urban, city, state, etc. and other factors.

Nevertheless, since cyberspace is anti-spatial, such characterization is not possible with regard to Cybercrime. As a result, pinpointing crime by location may be difficult. Understanding the motivations of cybercriminals is made possible by cybercriminology's examination of social characteristics and their geographic placements. For instance, if a larger percentage of cybercriminals come from low-income families or if Cybercrime appears to be more common in areas where poverty is endemic, then poverty may serve as a driving force behind Cybercrime.

### 2.1.1 Cybercrimes in organizations

Numerous companies now use various security measures to guard against being victims of Cybercrime due to the threat it poses. Financial security presents numerous issues for corporations, including banks and other similar establishments. Cybercriminals take advantage of a variety of methods, such as malware attacks that have the ability to take over a machine entirely and hacking. Organizations that allow hackers to get confidential information run the risk of going bankrupt or being blackmailed into giving the information to rival companies [13].

Cybercriminals can attack organizations using any internet application. A system can be attacked by a variety of worms and malware. Nonetheless, user IDs and information

can be obtained through conversations and mails. Cybercriminals have found that sending emails is a simple way to get access to computers and infect them with various viruses that can take down a domain's network system. Cybercriminals might leverage eye-catching and straightforward communications to compromise a system. According to Hamid [14], some of these viruses can spread without being launched in order to destroy and infect a system's whole database. Multiple assaults can be launched against security systems, which are typically considered active attacks, thereby jeopardizing the "hypertext markup language," or "HTML." It is possible to download more harmful software into a system in order to take control of it. Going online without an antivirus or firewall protection is extremely unsafe and dangerous for computer users. Cybercriminals employ a tactic called zombie attacks. This is accomplished by transmitting messages and information to other users via a different system acting as a host. These kinds of actions are typically conducted out for criminal motives; therefore, if the message's IP address and domain are found, an innocent person may be charged and classified as a cybercriminal.

This is typically accomplished by inserting a worm or virus into a victim's computer system (a botnet) and using the system without the user's awareness or attitude [15]. A 2009 BBC analysis of several studies on the "Botnet" revealed, based on journalistic accounts, that around 21,000 computer systems were used to blackmail e-commerce websites and send spam emails after becoming infected with malware. But it turned out that the majority of the compromised machines came from underdeveloped nations without access to adequate internet protection [14]. Nonetheless, the majority of businesses always have a robust firewall and antivirus program in place to ward off any intruding malicious assault that can bring down the entire company's system. Additionally, these firms employ experienced cyber computer engineers to monitor and guarantee the highest level of cyberspace security.

### 2.1.2 Cybercrime and the Study of criminology

Understanding the motivations behind crimes committed by people with certain characteristics, such as the number of offenders from a particular group of people who face discrimination in society, politics, the classroom, and the economy, is made easier by studying criminology. Furthermore, in traditional crime cases, social marginalization and geography are linked to crime, but this is not the case with Cybercrime. One important point to take into account is the fact that less people in

socially marginalized neighborhoods have access to the internet, which increases their likelihood of becoming involved in criminal activity. Furthermore, Cybercrime necessitates a certain level of information technology expertise and understanding. And from this vantage point, it is evident that cybercriminals seem to have greater privileges than the general public, having access to the internet. Therefore, findings the socioeconomic marginalization and criminality link that are relevant to traditional crime do not easily apply to Cybercrimes since they deviate from standards set for conventional crime. Thus, the existing perspectives linking social marginalization and prejudice as the driving forces behind crime do not apply to Cybercrime in the same way as they do to traditional crime. One of the biggest obstacles to state legislatures managing Cybercrime has been their inability to discern distinct motives [11].

### 2.1.3 The scope and nature of Cybercrime

In a community, crimes happen frequently. Living without experiencing traditional crime in the physical world is just as impossible as not experiencing Cybercrime in cyberspace. However, as time goes on, the kind and scope of criminal activity in a particular community shift. Therefore, a lot depends on the type of society in question when defining what constitutes a Cybercrime. This is true because the complexity of a crime in a society can be directly correlated with its complexity. In order to fully understand the characteristics of a criminal conduct in a community, Analyzing the various factors that affect and influence crime is crucial. Political, social, and economic aspects all play a part in comprehending Cybercrime and how best to address the issue through the implementation of appropriate solutions. When attempting to determine the type and breadth of a Cybercrime, it is also essential to take into account the preventative and corrective measures implemented by the mechanisms in place to control illicit activity within the specific community and Cybercrime [16].

The rise in Cybercrime has brought up new political, social, and economic issues. Furthermore, a lack of a clear legislative framework to address the crime as a result of a lack of knowledge about its nature and extent has given rise to even more complicated issues. Government apparatus and equipment are typically not up to date to recognize and manage the rise in Cybercrime. Information technology has widened the gap between countries and created a global village in terms of social, cultural, and economic spheres. One can reach the entire planet from one particular geographic point. Time and spatial boundaries have been disrupted by the development of contemporary

technology. It is difficult to effectively manage Cybercrime on a worldwide scale since cyberspace has no borders unlike the real world. Because Cybercrime is transnational, current equipment still cannot effectively manage it. The issue of criminals conducting Cybercrimes and evading detection has been brought about by the advancement of internet science and its vast prospects. Growing reliance on computer technology has made room for a growth in Cybercrime [17].

### 2.1.4 Cyber attack

Over the past few decades, the rise in cyberattacks has been a major cause for concern. Cybercriminals have employed a variety of cyberattack techniques to target consumers, including viruses, phishing scams, Trojan horses, worms, ransomwares, spyware, illegal access, and system control [18]. When a virus is connected to a program, it typically spreads to other systems. When a virus is run, the entire system can get corrupted. Phishing attacks are assaults that target social media platforms and often work by using a phony website link. When these links are clicked, a user's personal information may be revealed, providing a way for hackers to access passwords, credit card details, and user identities as well as other unauthorized databases. Trojan horses typically have hidden codes that, when activated, can take control of a machine and extract its data. Unauthorized access to a system or account is extremely dangerous, especially if financial information about the user is obtained [19]. Worm attacks are self-replicating infections that can infect host networks and propagate from one machine to another, overwhelming websites with traffic. Unlike viruses, worms propagate automatically throughout a system that doesn't require user execution; it doesn't need human execution. According to reports from European authorities, a ransomware known as "WannaCry" struck over 200,000 individuals and ten thousand organizations across approximately 150 nations. Typically, ransomware attacks a system by preventing users from having full access to it. These online criminals encrypt particular user data and applications, which they then demand to be unlocked in return for a cash ransom. Another kind of software that tracks a user's critical data is spyware. Emails, contact lists, and website logs can all be watched and utilized inappropriately in the future. Cybercrime can also include guessing or stealing someone's personal information in order to gain unauthorized access to a system. Moreover, it is possible to hack into a user's system to take control of its operations [20]. The anticipated Daily estimate of cyber-crime worldwide is displayed in the table below.

**Table 2:1**: Estimated daily global Cybercrime activity 2024 [20]

| Cybercrime | Daily activities |
|---|---|
| Phishing | 1 billion |
| Malicious attacks | 80 billion |
| Ransomware | 236.1 million |
| New malware | 106.8 million |
| Hacking | 35 billion |

## 2.2 Cybersecurity in Somalia

We must first examine how developed the ICT infrastructure is in Somalia in order to gauge the country's present degree of Cybersecurity awareness.

We will be able to determine the size of Somalia's attack surface thanks to the expansion of the ICT industry. We examine the Cybersecurity situation in Somalia and the measures that are in place. The risks Somalia faces and potential solutions to these issues are then discussed.

### 2.2.1 Overview of the ICT Infrastructure in Somalia

However, it appears that Somalia has a robust ICT infrastructure, primarily located in urban areas, especially the capital city of Mogadishu [21].

Internet users have increased in Somalia in recent years. In 2020, there were 1.63 million internet users, or 1.5% of the total population [22]. We are witnessing a trend in Somalia where increased internet access has resulted in a sharp increase in ICT usage. The most active economic sector in Somalia is ICT. It is one of the major components of the nation's annual GDP [23]. Local businesses have combined to grow the ICT industry [24]. Somalis can easily and affordably access ICT services since local businesses are expanding quickly [25]. The ICT industry has the potential to impact other industries by increasing profitability and productivity, which in turn attracts

investment. The nation as a whole, businesses, and individuals may all benefit from this digital opportunity, which will impact prosperity and growth.

The Internet Society's Somali chapter was founded in January 2011. Its objective is to encourage the Somali Community's quick adoption of the Internet and its related technologies. By educating IT professionals around the nation, it also raises awareness about Cybersecurity and internet security. It accomplishes this by starting programs like as Safer Internet Day Somalia, in which it disseminates knowledge about the safe use of the internet for social, commercial, and educational purposes. In November 2020, the Internet Governance Forum Somalia was initiated by the Somalia ISOC branch. Through debate facilitation, idea sharing, and exchange, this platform supports the ICT industry [25].

To encourage ICT in social and economic growth, the government has adopted the five-year "2019 - 2024, National ICT Policy and Strategy" [26] . The goal of this policy is to modernize the digital environment and create a more inclusive, knowledge-based society. This policy is organized as follows:

- Extend the reach of online shopping.
- Expand the use of internet media in the financial services industry.
- Promote R&D and digital literacy.
- Electronic governance in the fields of infrastructure, agriculture, and health.
- Extend network reach.
- Domain names, local hosting, Cybersecurity, and raising the caliber of services.

The National Communications Agency (NCA) was founded as the regulatory organization to safeguard Somalia's communications industry following the passage of the National Communications Law in 2017. Through the licensing of spectrum to businesses, they allow the government to generate cash. Additionally, they are creating several regulations, such as the Unified Licensing Framework [27].

- More than 20 telecom businesses are currently operating in Somalia, according to the Somali Economic Forum. Among the most well-known are Telecom, Amtel, Golis, Hormuud, and Telesom. The market is showing indications of innovation and entrepreneurship through the use of technology and commercial acumen [27]. Here are a few instances:
- Better Business Solutions is a consultancy that assists budding entrepreneurs with capital management, market research, and business plan development.

- Another online management tool, Guri Yagleel, attempts to make it easier for nationals to rent and own homes in the nation.
- The electronic payment system ePocket was chosen for the 2016 Innovate Accelerator program. By connecting banks, this application enables citizens across the nation to use the Internet to pay for school fees, utilities, and online shopping.
- Hormuud telecom, based in Mogadishu, introduced the Electronic Voucher Card Plus (EVC Plus). The use of this app facilitates transactions and transfers of mobile money.

### 2.2.2 State of Cybersecurity in Somalia

With the increasing use of the Internet throughout the world, Cybersecurity has gained national attention in Somalia. A large number of government functions and procedures are being done online. Cybercriminals utilize the internet to attack the commercial and public sector's sensitive assets in an effort to disrupt critical infrastructure and steal data from governments and citizens. These criminals have a variety of goals, including giving rivals intelligence information or making money. There isn't yet a well-defined Cybersecurity plan that can fend off widespread cyberattacks. Somalia is among the top 20 nations with the greatest percentage of infected computers, according to Kaspersky [28].

According to another report, hacking into official emails and web apps accounts for 80% of cyber incidents in Somalia. As a result, there is no detection system that can be employed to determine where the attacks are coming from. Some of the major cyberattacks that have affected Somalia during the past 10 years include hacking emails, personal computers, and web applications [29].

Major administrative and strategic decisions, such as establishing a national CERT (computer emergency response team) and putting in place a security awareness framework, are needed to improve the nation's security and guard against cyber events. It will be necessary to launch new projects and create new networks, such as those between government agencies and the police, between policy and private institutions, and between research institutions and commercial businesses [30].

Somalia does not yet have a national Cybersecurity strategy or directives, which include Cybersecurity frameworks, standards, rules, and awareness campaigns. Somalia's

ranking as one of the least cybersecure nations highlights the significant discrepancy between global norms and domestic Cybersecurity strategies. Cybersecurity education and training is not offered in any particular center in Somalia. Furthermore, according to Sambuli [31], there isn't a single platform where Somalians may learn about Cybersecurity concerns. Law enforcement officials and the legal system now have relatively little knowledge of Cybersecurity challenges, and there is a dearth of qualified Cybersecurity professionals.

Organizational policies pertaining to Cybersecurity, which is the activity of safeguarding information, should be strategically coordinated with cyber ethics, Cybersecurity, and safety protocols. Cybersecurity benefits and enhances a firm both as an entity and as a function. In addition to lessening the impact of stringent preventative controls, a business with a detection and response program in place will also be able to decrease the shadow of information technology, allowing for an increase in overall productivity within the organization [32].

In a same vein, a nation should establish strategic goals for safeguarding its vital IT infrastructure and populace at large. It ought to establish a special division tasked with creating and upholding the necessary Cybersecurity plans and procedures. In light of this, the NCA in Somalia serves as the official point of contact for SMEs, public authorities, ICT providers, Internet service providers (ISPs), individuals, and providers of vital infrastructure [(NCA, 2018)]. Its extensive national mandate includes creating national Cybersecurity plans and increasing Cybersecurity awareness across the nation. Additional goals include of:

- Overseeing the duties assigned to SomCERT/CC
- Identify, prevent, and handle negative cyber events; this includes providing guidance and creating the required regulations.
- Oversee and direct the reaction to severe conditions resulting from malevolent cyber occurrences.
- Examine and certify Cybersecurity procedures used to safeguard IT systems and goods.
- Encourage operators of public services and vital infrastructure to comprehend and abide by Cybersecurity regulations in order to increase awareness of Cybersecurity nationally.

To safeguard, monitor, and secure Somalia's significant cyber assets and cyberspace, a Cybersecurity department was established together with the National Communications

Agency. Although it is not required by law, all Cybersecurity events must be reported to the NCA [2018]. A Computer Emergency Response Team was formed in May 2019 within the National Communications Agency's Cybersecurity division. Its primary goal is to give every Somalian access to a more robust and safer internet. The official website states [Som-CERT, 2018]. They plan to offer the following:

- Providing government agencies with intrusion detection and prevention systems.
- Providing government organizations and owners of vital infrastructure with information about Cybersecurity awareness.
- Responding to cyberattacks that occur in Somalia.
- Strengthening Somalia's Cybersecurity posture through collaboration with other CERTs worldwide

On their website, the Somalia CERT posts instructions and alerts; nevertheless, to reach a larger community, they do not have a Cybersecurity awareness plan. Additionally, they are not active on social media, which means they are losing out on a significant opportunity to connect with more people.

The CERT team's capacity to collaborate with the different nations affiliated with these entities is greatly enhanced by its membership in Africa-CERT and OIC-CERT (Organization of the Islam Countries – CERT). But it should also aim to become a member of other global security teams, such as FIRST (Forum of Incident Response and Security Teams). As a result, Somalia CERT will have more opportunity to collaborate with other CERTs, develop its capacity, and have access to a wealth of information that will help it improve its response skills [Som-CERT, 2018].

### 2.2.3 Obstacles facing Somalia

Amidst decades of strife, an externally focused, transparent, and relatively deregulated economy has thrived [33]. Aspiring businesses have given Somalis means of transferring and receiving money. Additionally, there has been a rise in the diaspora of Somalians investing more money back home. This has made it possible for the ICT industry and telecoms firms to function well.

Vulnerable systems and a lack of Cybersecurity standards may be the cause of cyberattacks in Somalia. Cheap and widely available are software programs that have been pirated. Malware spreads because this security software cannot be updated from

the versions provided by the vendor [34]. Without proper security measures, the rise offers more access to cyberspace. Controlling implementations in cyberspace, enforcing laws, and regulating authorities are all made feasible by a strong regulatory framework. In the absence of this, Internet usage would suffer and Somalia's rate of Cybercrime would rise.

Financial crimes are common in Somalia. The government is unable to control and settle financial conflicts, such as frauds, erroneous transactions, or disagreements over the amount of the transfer, because there are no official banking or regulatory frameworks and complicated relationships amongst the courts [35]. The nation's legal system needs to be significantly enhanced in order to handle electronic evidence and Cybercrime. A major problem in this case is the ignorance and incompetence of judges and prosecutors in particular; they need to receive specialized training.

Due to Somalia's inadequate ICT infrastructure, sensitive data from both public and commercial institutions is frequently compromised. It suggests that the national agencies tasked with responding to and resolving cyber-related concerns are not yet developed enough to be able to do so. Law enforcement and inadequate regulations are other issues in the nation. The rapid expansion of communications businesses and the industry's success in the absence of official regulation have both contributed to Somalia's stabilization and created an environment that is conducive to Cybercrime [36].

An additional obstacle for ICT and cyberspace in Somalia is the extremist organization known as Al-Shabab. Al-Shabaab-controlled areas have severely restricted ICT use and outlawed Internet access, citing it as un-Islamic, making rules and laws harder to implement. But in order to further its cause, the party uses social media, which could put its neighbors at risk. Al-Shabaab has given the nation a fresh set of challenges and issues. The employment of new technology and the possible threat of cyberattacks have been considered seriously by anti-terrorism operations [31].

Somalia receives insufficient funds for Cybersecurity. As a result, institutions and citizens are less able to keep an eye on and monitor Cybersecurity in the nation. Many African nations view Cybersecurity as an extravagance rather than a necessity. Its importance is still not fully understood or acknowledged. Many organizations are projected to spend less than 1% of their budget on Cybersecurity [37]. Resources must be added to improve cyber threat detection and incident response capabilities.

The incapacity of Internet users to protect themselves against cyberattacks is another issue. The majority of Internet users lack technical competence and are inexperienced. There is a severe lack of skilled labor in the nation. Lack of experienced IT staff makes many organizations, particularly government institutions, more susceptible to Cybercrime [38] In the realm of Cybersecurity, knowledge and technical education are required. To strengthen Somalia's online, capacity building campaigns ought to be implemented to empower the populace.

It's probable that Somalia lacks a strong Cybersecurity competence because the organizations addressing the issue are still in the early phases of development. Cybersecurity is an ongoing process rather than a single stage. Thus, lawmakers, lawyers, the courts, the intelligence community, the public, young people, the media, civic society, and the military should all take an active role in attempts to address Cybersecurity as soon as feasible in addition to drafting legislation. In order to comprehend the issues and procedures involved, it is imperative that all stakeholders are included [39].

Networks of police and government agencies, police-private, and foreign-police should all be required to evolve as standards for computer networks. Additionally, all Cybercrimes involving digital technology must to be included. [30].

## 2.3 Theoretical Framework of The Study

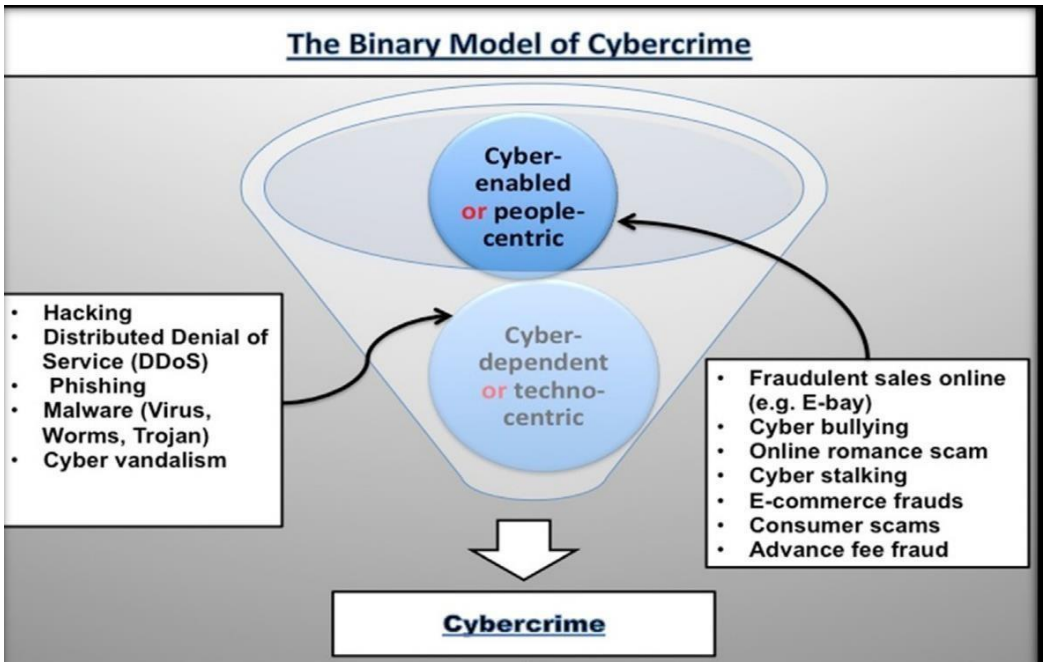
The Protection Motivation Theory (PMT) serves as a theoretical framework for this study. The PMT, which was introduced by Rogers in 1975, describes actions intended to safeguard the agent of action in response to both internal and external factors. In reaction to threats or pleas for fear, people typically behave protectively, using both emotional and logical strategies, according to PMT. Threat assessment and coping appraisal are two different processes that are involved in dealing with these threats or fear appeals [40]. According to Rajab and Eydgahi [41], threat appraisal comprises the subjective evaluation of danger severity, probability, and individual susceptibility. Assessing one's ability to adjust to the threat and one's own perceptions of competence, responsiveness, and self-efficacy in handling it are all components of coping evaluation [41]. When integrated, PMT provides a structure for explaining the primary and secondary procedures that organizational leaders use to understand and handle

Cybersecurity vulnerability, cyber hygiene, and information security policy compliance (ISPC).

The purpose of this study is to determine the institutional and individual elements that influence an organization's Cybersecurity risk; hence it is imperative that the theoretical framework underlying these variables be validated. Because PMT integrates internal cognitive-emotive elements (such individual beliefs and knowledge) and external institutional factors (like repercussions and possibility of harm), it is frequently used in this setting [41]. Prior studies, including those conducted by Choi [42] and Hina [43], have shown how useful PMT is for examining institutional and individual aspects of Cybersecurity and ISPC compliance. For example, Hina [43] confirmed qualitative correlations between ISPC and institutional governance, and Choi [42] demonstrated a qualitative relationship between organizational Cybersecurity and insider beliefs.. To summarize, the alternative hypothesis put out in this study is supported by research on Cybersecurity and ISPC using PMT.

### 2.3.1 A dual mode of Cybercrime

As Ibrahim [44] suggests, the phrase "Cybercrime" refers to several internet transgressions, such as those performed through computers, computer networks, or other ICTs. Cyber fraud and other cyber-enabled crimes, however, "can still be committed without the use of ICT00." Figure 2.1 provides an illustration of these dual groupings. In contrast to conventional crimes, a single Cybercrime scheme has the



potential to affect numerous countries at the same time, entail numerous actors, and involve various states.

**Figure 2:1**: Cybercrime Binary model [44].

### 2.3.2 The value chain of Cybercrime

According to Tang and Rush [45], value chain analysis includes every necessary action taken in delivering a product or service from the beginning to the last stages of production and ultimately to the consumers. Although the relationships depicted in a value chain could generally appear more vertically within a single type commercial product than the notion of a company natural system, which reduces on a level plane cross-wise over multiple divisions, items, and officials, Value chains also relate to the contributions made by a variety of fictional characters in various businesses.

Eventually, the concept of noteworthy value chains offers important contributions to comprehending the surroundings since, among other things, it identifies certain characters on screen in the value chain and illustrates how their positions change over time. Secondly, it identifies the fundamental sequence of tasks necessary for the creation of projects and goods. Thirdly, it differentiates the connections among the various workouts in the sequence. Fourthly, it motivates us to identify the strong and weak ties and observe who benefits throughout the production network. In the end, it makes a difference in terms of who takes on a major role in its success or how it is managed. Finally, it highlights the importance of modernizing or enhancing skills and framework, services, and products.

In this sense, a value chain structure provides tidbits of information about the components of a corporate biological system. Cybercriminals compete and plan their actions to get an advantage over a specific market segment, much like in the real world of business. The above-depicted series of tasks necessary to create a product or service involves combining the contributions of various on-screen characters, who are frequently gradually distributed around an organization. One of the main concerns of a thorough value chain analysis is to enhance understanding and decompress the relationships between the performers involved in the range of activities that result in the creation of a competent management.

Each exercise by various performers is suggested to assist the unidentified age of financial advantage. Consequently, each movement can be linked to different strategies

for turning a profit in their own niche markets, sources of advantage and profits, or value-added benefits, which combine to form a value chain. Thus, Cybercrime can be seen as a whole value chain that promotes deception, with a variety of activities, net profits, creative abilities, and the redesigning of goods and services, and, eventually, opportunities associated with each step.

Three basic exercises can be identified within Cybercrime value chains that result in charge card deception and wholesale fraud: (1) identification of computerized systems' vulnerabilities, such as those accessed via the internet; (2) propagation and system infection; and (3) abuse of the flaws in the syste

# Chapter 3
# METHODOLOGY

## 3.1 Introduction

An overview of the study methodology, including the strategy, study model, papulation, as well as sample techniques, is given in this chapter. It goes over the tested hypotheses and the data gathering methods used in the study. Furthermore, techniques for ensuring validity and dependability were discussed, as well as methods for data collecting and analysis. Additionally, ethical issues surrounding this research were covered.

## 3.2 Approach

For this study, I have selected the research category of quantitative methods. According to Leedy and Ormrod [46] and Sallis [47] quantitative techniques are broadly described as a class of research methodologies that are defined by the collecting of information that is amenable to mathematical quantification. Measurement, observation, surveys, questionnaires, interviews with quantitative components, document collection, artifact collecting, or the use of pre-existing quantitative datasets are some methods that can be used to gather data for quantitative studies [48]. In quantitative research, data gathering may also entail sophisticated methods including deception, blinding, and the use of control groups [48]. These methods are used to achieve certain methodological objectives, such heightened rigor, establishing causality, or meeting particular study objectives [48]. All quantitative approaches share the trait of quantifiable data and the variety of ways in which they can be gathered.

The complexity of quantitative approaches can vary significantly based on the study's objectives and the data that needs to be gathered. When conducting a simple quantitative study, data that is easily comprehensible, contextualized, and organized is gathered and analyzed using descriptive statistics, such as distribution, and frequency ( [46],[49]). Using more sophisticated inferential statistics, combining inferential and descriptive statistics, or collecting and analyzing numerical data to determine quantifiable relationships between variables are some examples of more complex quantitative methodologies ([47],[46]). In conclusion, research involving statistical analysis of numerically measurable variables are best served by quantitative approaches.

My examination of the literature indicates that, while to differing degrees of methodological complexity, quantitative approaches were used in the majority of Cybersecurity research from 2017 to 2024. The information technology industry has a general bias in favor of large-scale datasets and statistical analysis like the CSBS are now more publicly accessible, and prior qualitative investigations have already finished much of the exploratory work, which is why quantitative methods are so popular ( [51]-[53]). Studies that use descriptive statistics to explain and put the quantitative aspects of the problem under study in context at the least amount of statistical complexity possible, such as the Angraini [51]. research analyzes simple, information-rich survey data. Most studies cluster around the middle complexity, where descriptive statistics provide context for the inferential statistics used to confirm or refute causal or correlational connections among a limited set of variables ( [54]-[57]). The most complex studies are those that are ambitious and large-scale, like those by Moody [53]. and Koohang [52]., where researchers use several different inferential statistics modes in multiple iterative steps to accomplish complex research goals, like developing or validating a unified theoretical framework of ISPC. Quantitative approaches are the most popular study strategy, and it is evident that they have been successful in shedding light on insider threat and ISPC challenges in the Cybersecurity space.

For this study, I decided to evaluate the primary dataset using a quantitative methodology. The gathered dataset was the main reason why the quantitative method was the most suitable. The fact that this study's features made the quantitative approach the most suited choice for this technique also made sense. The necessity for a reliable theoretical framework to test hypotheses, variables that can be measured quantitatively, and a representative sample to guarantee the results' generalizability are the main drawbacks of quantitative data analysis [47]. However, while maintaining the overall rigor of this study, these flaws were immediately addressed by the application of protection motive theory and a methodologically sound archival dataset. As with any quantitative analysis, there was no assurance that any statistically significant associations between variables would be discovered, but this was not viewed as a flaw [46].

In conclusion, the dataset was best analyzed utilizing quantitative approach with PMT serving as the main theoretical foundation.

## 3.3 Population and Sampling

### 3.3.1 Population

The study's population included both private businesses and non-profit organizations. operating in Somalia; all of which operated in industries where Information Technology is indispensable. The survey sought to capture the Cybersecurity risk profile across different sectors and on organizations that had fully adopted IT in their business processes.

The sample population was developed from the Somalia's Department of Business Register with a list of 380 business. Educational institutions, both public and private, at all levels from the primary school to the university were also taken into consideration. The participants were purposively selected to consist of leaders of the highest rank within an organization, whose responsibility is to oversee Cybersecurity. Companies that did not fit the criterion of possessing IT and a certain size were omitted to make this research applicable to Cybersecurity. The population data was then traced and cleaned to make the eligible population comprises of 40 business and 22 educational institutions. Companies were grouped according to the number of employees as follows; micro enterprises with 1-9 employees, small enterprises with 10-49 employees, medium enterprises with 50-249 employees and large enterprises with 250+ employees.

Despite the failure to review the total population of Somalia, the study used registered businesses as the usable population and was quite reasonable.

### 3.3.2 Sampling

The selection of the sample was done purposively in a way that ensures maximum variation and include active organizations within the Cybersecurity field. Only organizations with more than two people employed for them were used to guarantee that their focus concerns Cybersecurity cooperation only. Sole traders were not considered since there is usually no combined IT support system. Companies in which IT plays a significant role and Cybersecurity constitutes a key issue were selected more specifically. Organizations working in the public sector and those working in the fishery, forestry, and agriculture industries were excluded due to their considerably different Cybersecurity expectations and authorization procedures.

To achieve a minimum level of bias in the sampling procedure and to maximize the generality of the conclusions the study intended to select the participants most similar

to a true random sample. To make the study well representative, the researcher used a stratified random sampling design. This was very useful in helping the investigator capture all the extreme values and make sure that each sub category of business was represented in proportion in the sample. Some of the subgroups among the organizational types were provided with a higher likelihood in order to balance any possible oversample.

The final was chosen out of 32 organizations qualified and suitable for the study that helped the researcher to provide an understanding of the state of Cybersecurity for Somali businesses and educational facilities.

### 3.4 Research Model

The study model is founded on a theoretical framework that investigates the connection between attitudes regarding Cybersecurity and Cybercrime and demographic characteristics such as gender, age, position at work, and experience.

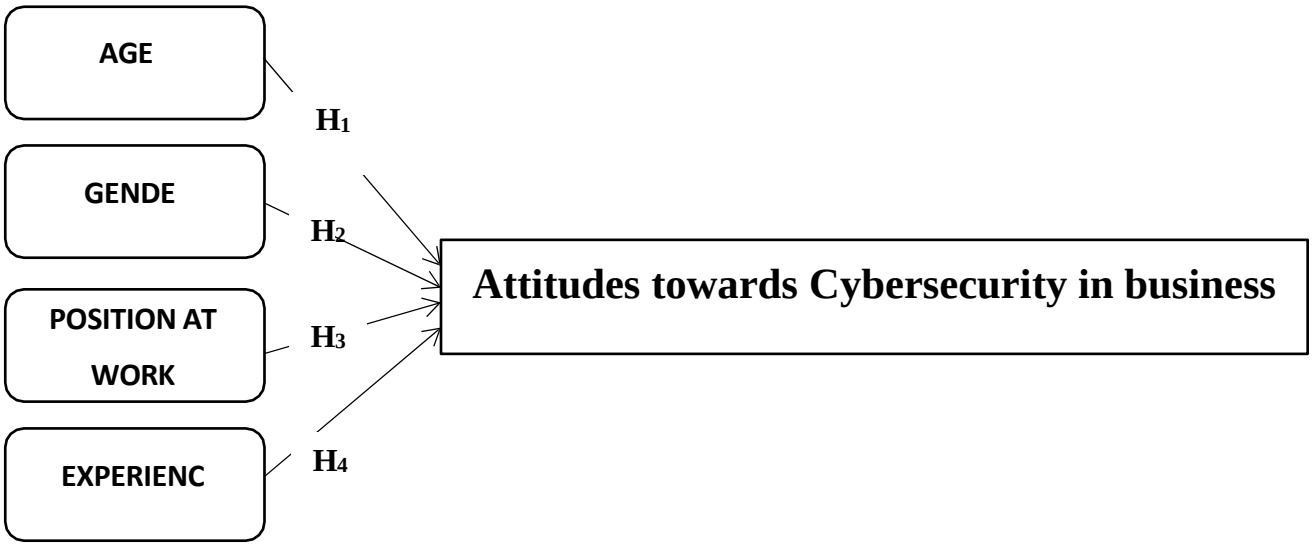



**Figure 3:1**: Research model [58].

### 3.5 Hypothesis

Throughout the investigation, several hypotheses will be examined in order to examine Cybersecurity-related problems in Somalian organizations. Below is a list of them:

- H1: There is a significant correlation between employees' age and their attitude towards Cybersecurity or Cybercrime
  H0: There is no significant correlation between employees' age and their attitude towards Cybersecurity or Cybercrime

- H2: There is a significant correlation between employees' gender and their attitude towards Cybersecurity or Cybercrime.
  H0: There is no significant correlation between employees' gender and their attitude towards Cybersecurity or Cybercrime.

- H3: There is a significant correlation between employees' position at work and their attitude towards Cybersecurity or Cybercrime.
  H0: There is no significant correlation between employees' position at work and their attitude towards Cybersecurity or Cybercrime.

- H4: There is a significant correlation between employees' Experience and their attitude towards Cybersecurity or Cybercrime.
  H0: There is no significant correlation between employees' Experience and their attitude towards Cybersecurity or Cybercrime.

### 3.6 Data Collection

The researcher used a survey research approach to collect the data for this study and specifically utilized a structured survey questionnaire in the form of an online Google Forms. This was preferred since it is easy to use hence enabled the gathering of responses from the workers in the different organizations in Somalia. The questionnaire was administered to a heterogeneous workforce in various areas in the organizations listed in the earlier named companies. This was to ensure that the ideas collected covered a wider view of what the workforce needed in terms of the challenges it faced and the solutions available. Wide coverage and follow up response rate helped in acquiring a substantial dataset of valid and completed surveys.

The questionnaire was thoughtfully split into two separate sections: Section A: the details that were collected under this part include age, gender, department, details of the person's working responsibilities and years of service with the organization. Such information is helpful to analyze the context of the replies and detect any tendencies regarding demographic factors in Cybersecurity concerns and behavior. Section B: The second part of the survey was based on the one-dimensional attitudes towards Cybersecurity in business model (ATC-IB) by lee [58]. The tool was based on approximately twenty-two selectively developed questions in order to assess the employees' attitude towards Cybersecurity measures. The questions covered different aspects of Cybersecurity concerns, including: whether individuals are responsible for Cybersecurity within their organizations, and whether the organizations' existing rules are effective; and how Cybersecurity influences the everyday operations within organizations.

The survey questions were structured using the 4-Point Likert scale, which ranged from strongly disagree (response point 4) to disagree (response point 3) to agree (response point 2) to strongly agree (response point 1). Since there was no equivalent 'middle ground' option, this scale was created with the purpose of measuring the intensity of the valuation expressed by the employees on this particular attribute while at the same time putting them into a corner and talking more about their attitude.

Consequently, the main goals of this survey were to determine ideas of the actual impact of workers' perception of Cybersecurity at their organizations. The following outlined research questions seeks to achieve the given objective: The research questions are as follows; What are the attitudes that are likely to influence the effectiveness of Cybersecurity measures in Somalia's corporate world?

### 3.7 Reliability and Validity

A reliability test was carried out to guarantee the accuracy and consistency of the survey instrument utilized in this investigation. This test was intended to ascertain the internal consistency of the questionnaire items, namely those intended to gauge respondents' opinions toward Cybersecurity.

One well-known statistical method used to evaluate the survey's reliability was Cronbach's alpha. This coefficient calculates the degree to which a group of elements,

or questions, have a positive correlation with each other, resulting in a scale that accurately assesses an underlying concept. Higher Cronbach's alpha values (between 0 and 1) indicate higher degrees of internal consistency. It is common to classify an alpha of 0.9 or higher as exceptional, 0.8 or higher as good, 0.7 or higher as acceptable, 0.6 or higher as questionable, 0.5 or higher as poor, and less than 0.5 as inadequate. After examination, the survey's Cronbach's alpha was determined.

The outcome supports the validity of the questionnaire and will be covered in more detail in the sections that follow. While a lower alpha might indicate that certain questions need to be revised to increase the reliability of the scale, a high alpha coefficient would indicate that the survey items consistently represent the participants' opinions regarding Cybersecurity. An essential stage in verifying the survey instrument is the reliability test. It guarantees that the questions are arranged so as to precisely and unambiguously capture the required information. Since these measurements serve as the foundation for further data analysis and interpretation of the workforce's viewpoints on Cybersecurity measures in Somalia, the study's credibility depends on how reliable these measurements are.

**Table 3:1** Result reliability test

| **Dimension** | **Cronbach's Alpha Reliability** |
|---|---|
| ATC – IB | 0.983 |

### 3.8 Data Analysis

To ensure that the data we collected was clean before analysis, some data cleaning was done on the data collected. These measures entailed a process of data analysis to detect and remedy missing values, outliers, and inconsistencies. I also realized that there was an occurrence of invalid or incomplete questionnaires during this process. The following relevant variables were built through survey items: −These variables reflect various aspects of the attitudes towards cyberspace. After entering the data into the social science statistical tools (SPSS), the scholar saw that some questions were missing some information or they were not completed at all. Some of the questionnaires which were only partially filled were identified and set aside for closer study. In a bid to maintain a high data quality, all the incomplete questionnaires were rejected from the analysis. In addition, only valid and complete responses were used for the next step.

Frequency and percentage distribution were employed to examine the demographic characteristics. This included structural features such as age, gender, and roles held in the workforce. A good understanding of the composition of the workforce is critical when addressing issues of attitude towards Cybersecurity.

Independent t-test Established whether attitude towards Cybercrime/Cybersecurity significantly differed based on gender. For instance, it evaluated the differences in the perceptions that male and female employees had.

The present study used Pearson's correlational analysis to determine the ways in which variables are related. In more detail, it investigated the relationship between the age of employees and their perceptions of Cybercrime as well as Cybersecurity for the business.

To determine the effect of Work Position, analysis of variance one-way ANOVA test was carried out. It involved collection of data from the sub-group categories of employees (junior staff, middle management, senior executives) on attitudes. It seeks to determine if employees from various positions have distinct opinions regarding Cybersecurity.

A further 1-way ANOVA looked at how work experience affected the attitudes. Was there a difference in the perceived threat of cyber threats between employees with different tenure? These analyses will serve as the foundation for the study's conclusions. The general outlook of the workforce determines the validity of the policies and training to be implemented in the cycle in Somalia.

### 3.9 Ethical Considerations

Ethical considerations for the participants were clearly prioritized in this thesis, and those considerations were followed here. Each study has its own unique set of ethical considerations that must be taken into account during the planning and design phases. There is no one "formula" for ethical behavior, but research should always act in a morally responsible manner. Among these tenets are fairness, candor, integrity promotion, respect, and risk assessment analysis to keep participants safe. Researchers should also protect participants' anonymity by obtaining their written informed consent after explaining the study's optional nature. Furthermore, the ethics of research and thesis work at universities should be consistent with the ethos of the respective

institutions. In this scenario, the supervisor was consulted about the study's approach to guaranteeing conformity to these standards. Certain measures were put in place to guarantee adherence to these moral guidelines. Subtly and politely a month before the event, participants were contacted through email and given the option to participate on dates that were most convenient for them. The researchers did not tamper with the data and made sure it fairly represented the individuals' experiences. The researchers thanked them for their help and said they would take all necessary precautions to protect their data and personal information [59].

# Chapter 4
# DATA ANALYSIS AND RESULT

## 4.1 Introduction

The outcomes of the study and interpretation of the data on Cybersecurity awareness measurement in Somalian organizations are presented in this chapter. The data were processed and presented in accordance with the goals and reliability of the study. I utilized tables to show the distribution of replies to different questions in order to demonstrate. Frequency, percentage, and correlation analysis were utilized to display and evaluate the data that was gathered in order to explain, analyze, and make conclusions. I disseminated Google Forms questionnaires, and I got 156 replies in all. Every inquiry had a proper response. The population statistics data were analyzed using descriptive statistics from the Social Science Statistics Package 29 (SPSS). Respondents were asked questions on their gender, age, years of experience, position within the business, and degree of education in the demographic profile section of the survey

## 4.2 Data preparation and cleaning

To ensure the accuracy and consistency of the data you work with, and structured appropriately, Cleaning and preparing data is a crucial stage in the data science process. Just to refresh your memory, I said that Google Forms has collected 160 "submitted" replies, of which 156 were legitimate (the other four were either blank or inadequate).

## 4.3 Research Respondent’s

The research was carried out in the spring of 2024. Workers were chosen from eleven Hargeisa-based Somalian organizations. Participating companies included Premier Bank, Dahabshiil Bank, Dara-salaam Bank, Telesom Company, Somtel Company, and others.

There are 156 workers that are taking part in this study. Every research participant provided their best honest and nonreligious response to the questions.

### 4.3.1 Respondent's demographic data

An individual's gender can have a big influence on their attitude and ability to make decisions [60]. Put differently, a number of researches considered gender to be a significant aspect that influences the intention of some consumers.

The research of customers' perceptions of new literature information also recognizes age as a critical factor, although one that has to do with Cybercrimes rather than just technology. [60].

demographic information that would be displayed as a frequency table.4.1. It displays the information from the individuals who actively contributed to this study.

**Table 4:1** Research Respondent's demographic

| **Demographic Variables** | | **Frequency** | **Percentage (%)** |
|---|---|---|---|
| Gender | Male | 92 | 59.0 |
| | Female | 64 | 41.0 |
| | Total | 156 | 100.0 |
| Age | 23 – 60 years | | |
| Level of Education | High school | 18 | 11.5 |
| | Bachelor | 123 | 78.8 |
| | Master | 15 | 9.6 |
| | Total | 156 | 100.0 |

**Figure 4:1** Participant's Gender

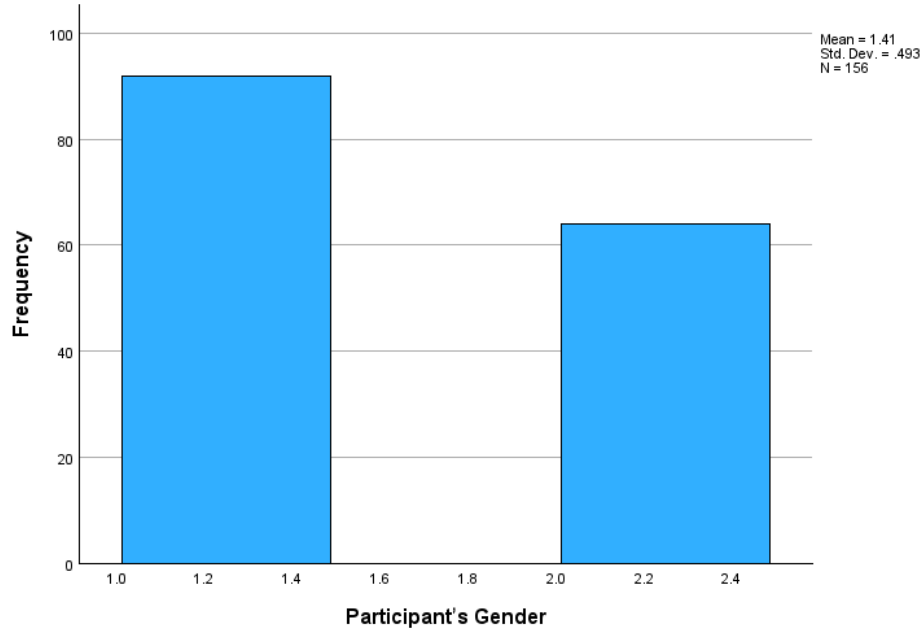



**Figure 4:2** Participant's Age

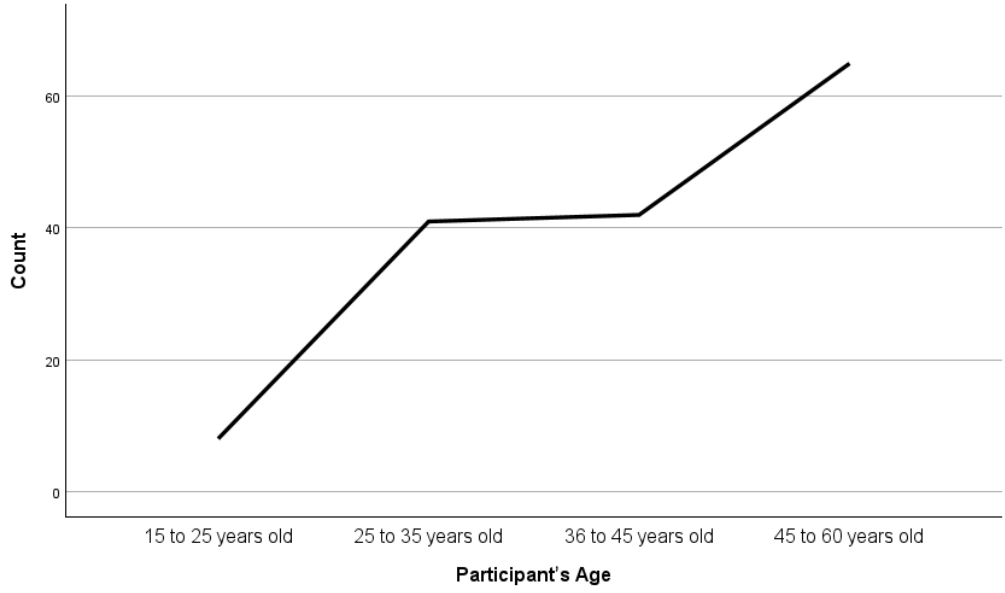
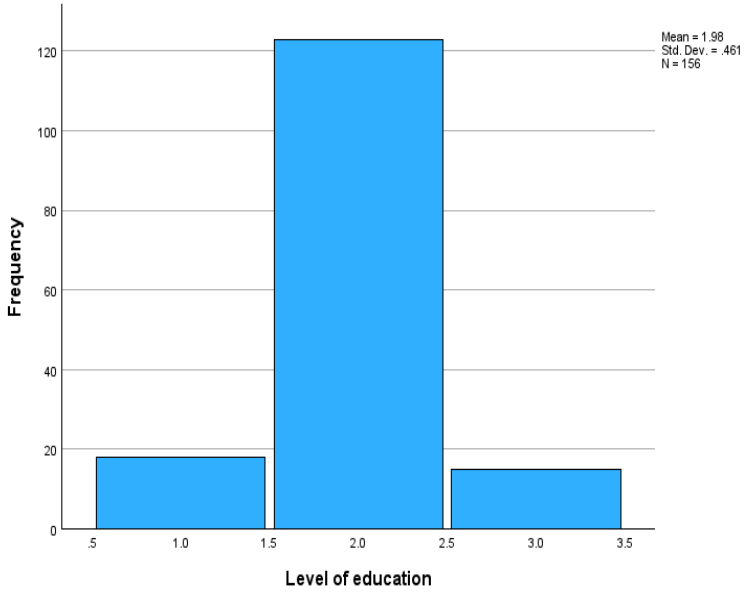


**Figure 4:3** Level of Education




Males participated numbered around 92, with a corresponding value of 59.0%, while females have 64 frequencies, and a percentage of 41.0%. Given that participants are workers who represent companies, their ages ranged from 23 to 60. The greatest level of education acquired by those personnel was a master's degree. 123 employees (78.8%) had a bachelor's degree, 15 (9.6%) had a master's degree, and 18 (11.5%) were all high school graduates.

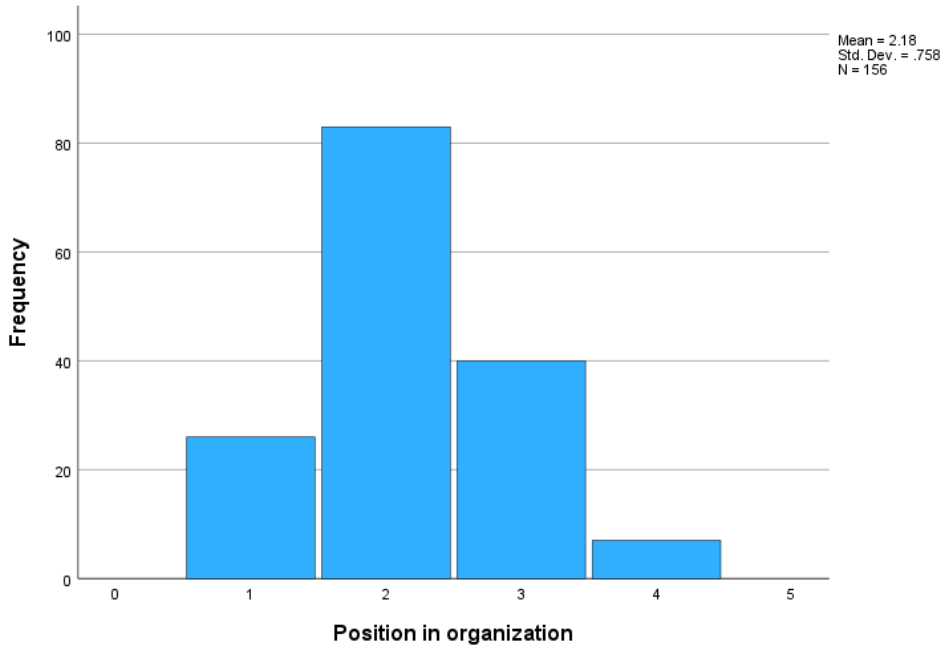
### 4.3.2 Position at the organization

According to Table 4.2's results, around 6.4% of them had a frequency of 10 and were managers; 17.9% had a frequency of 28 and were supervisors in the organization; 47.4% had a frequency of 74 and were once again senior laborers; and the last, but most certainly not least, was a junior laborer, who had a frequency of 44 and 28.2% percent.

**Table 4.2:** Position at the organization

| Positions | Frequency | Percentage (%) |
|---|---|---|
| Manager | 10 | 6.4 |
| Supervisor | 28 | 17.9 |
| Senior Laborer | 74 | 47.4 |
| Junior Laborer | 44 | 28.2 |

**Figure 4:4** Position at Organization



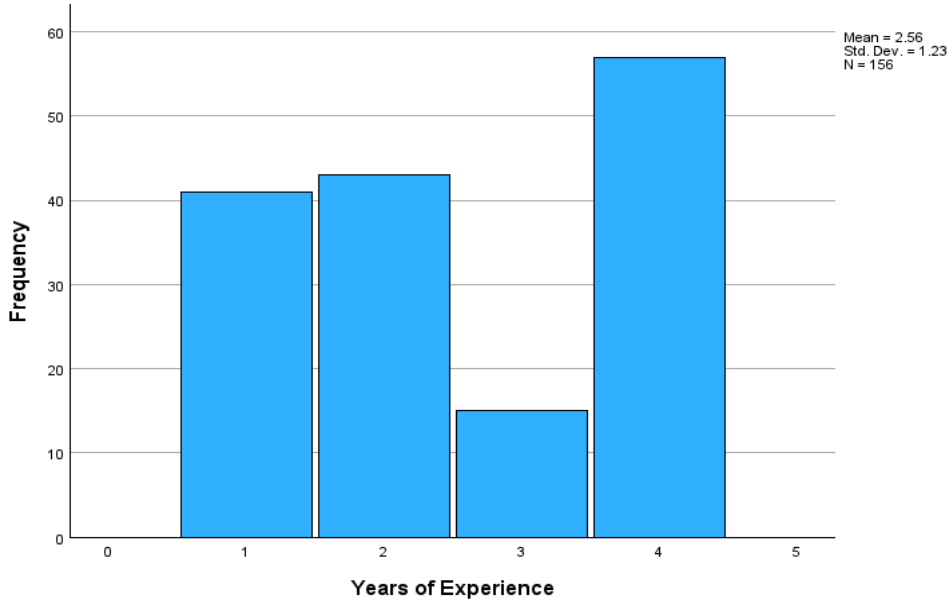

### 4.3.3 Years spent working for the company

Table 4.3 illustrates the results obtained from the reported data, which indicate that 26.3% of the workforce has worked for the organization for less than five years, 27.6% for five to ten years, 9.6% for ten to fifteen years, and 36.5% for fifteen years or more. Again, 156 employees actively engaged in this portion of the survey, which was completed during business hours.

**Table 4.3:** Years spent working for the company

| Years spent | Frequency | Percentage (%) |
|---|---|---|
| Under five | 41 | 26.3 |
| Between 5 - 10 | 43 | 27.6 |
| Between 10 - 15 | 15 | 9.6 |
| 15 – above | 57 | 36.5 |

**Figure 4:5** Years of experience




## 4.4 Attitude of employees

This section's examination will address each verdict in light of the previously stated hypothesis. The replies provided by the respondents (employees) in these businesses, together with their individual responses to the questionnaires concerning there "attitude towards Cybersecurity in business," is also being examined.

**Table 4.4: Scale items for the ATC-IB questionnaire**

| Items | SA % | A % | D % | SD % | M | SD |
|---|---|---|---|---|---|---|
| It is the management's duty to guarantee that a business is secure against Cybersecurity threats. | *48.7* *(76)* | *50.0* *(78)* | | *1.3* *(2)* | *1.54* | *.572* |
| I believe my responsibility is to keep the organization safe from possible cybercriminals. | *3.8* *(6)* | *3.8* *(6)* | *70.5* *(110)* | *21.8* *(34)* | *3.10* | *.634* |
| Every employee in the company has a responsibility to defend it from hackers' attacks. | *27.6* *(43)* | *66.7* *(104)* | *3.8* *(6)* | *1.9* *(3)* | *1.80* | *.595* |
| It's difficult to say how I can contribute to the organization's Cybersecurity protection. | *12.8* *(20)* | *69.9* *(109)* | *13.5* *(21)* | *3.8* *(6)* | *2.08* | *.642* |
| lack of the necessary abilities to defend the company from Cybercrime. | *13.5* *(21)* | *67.9* *(106)* | *14.7* *(23)* | *3.8* *(6)* | *2.09* | *.656* |
| IT security is not a priority for my company. | *7.7* *(12)* | *23.1* *(36)* | *39.1* *(61)* | *30.1* *(47)* | *2.92* | *.916* |
| Computer systems are capable of providing an organization with all the protection it requires. | *15.4* *(24)* | *56.4* *(88)* | *22.4* *(35)* | *5.8* *(9)* | *2.19* | *.760* |
| I feel like Cybercrime reports are pointless. | *5.1* *(8)* | *32.7* *(51)* | *42.9* *(67)* | *19.2* *(30)* | *2.76* | *.820* |
| The authorities are ill-equipped to handle Cybercrime efficiently. | *25.0* *(39)* | *65.4* *(102)* | *4.5* *(7)* | *5.1* *(8)* | *1.90* | *.702* |
| Cybercriminals, in my opinion, are more sophisticated than those who are meant to be keeping us safe. | *26.9* *(42)* | *64.7* *(101)* | *5.8* *(9)* | *2.6* *(4)* | *1.84* | *.638* |

**Table 4.4: Scale items for the ATC-IB questionnaire continued.**

| Items | SA % | A % | D % | SD % | M | SD |
|---|---|---|---|---|---|---|
| Notifying the police of a cyberattack might damage the company's reputation. | 11.5 (18) | 76.9 (120) | 10.9 (17) | 0.6 (1) | 2.01 | .502 |
| There is more that can be done to educate employees about the risks posed by Cybercrime. | 6.4 (10) | 3.8 (6) | 75.6 (118) | 14.1 (22) | 2.97 | .662 |
| The organization's utilization of IT strategy is known, and efforts are made to adhere to it. | 0.6 (1) | 9.6 (15) | 78.2 (122) | 11.5 (18) | 3.01 | .489 |
| If there was a cyberattack, I would have no idea how to notify it. | 12.2 (19) | 73.7 (115) | 10.3 (16) | 3.8 (6) | 2.06 | .614 |
| I don't believe it is my duty to notify the organization of a cyberattack. | 7.7 (12) | 54.5 (85) | 27.6 (43) | 10.3 (16) | 2.40 | .777 |
| If dangers from Cybercrime harm material for an organization, that is not my problem. | 8.0 (14) | 47.4 (74) | 31.4 (49) | 12.2 (19) | 2.47 | .822 |
| I'm sure I could recognize the warning indicators of a cyberattack. | 7.1 (11) | 25.0 (39) | 62.8 (98) | 5.1 (8) | 2.66 | .686 |
| The greatest risk to IT systems, in my opinion, comes from employees. | 5.8 (9) | 12.2 (19) | 71.2 (111) | 10.9 (17) | 2.87 | .669 |
| I believe that anyone working for the organization might be manipulated by arrogant scam artists. | 3.8 (6) | 3.8 (6) | 77.6 (121) | 14.7 (23) | 3.03 | .584 |

**Table 4.4: Scale items for the ATC-IB questionnaire**

| Items | SA % | A % | D % | SD % | M | SD |
|---|---|---|---|---|---|---|
| Cybercriminals find it easy to attack an organization that has a notable increase in revenue. | 19.9 (31) | 69.5 (114) | 7.1 (11) | | 1.87 | .504 |
| Cybercriminals only target big organizations. | 17.3 (27) | 75.0 (117) | 7.1 (11) | 0.6 (1) | 1.91 | .513 |
| I'm not sure who is responsible for keeping the organization safe from cyberattacks. | 13.5 (21) | 63.5 (99) | 17.3 (27) | 5.8 (9) | 2.15 | .720 |

Note: SA = Strong Agreed; A = Agreed; D = Disagree; SD = Strongly Disagree; % = Percent; M = Mean; SD = Standard Deviation.

The table above shows the frequency and valid percentage of each questionnaire-filled participant based only on whether they (SA, A, D, DA) with each question regarding participants' attitudes toward Cybersecurity and cyber-crime in general when it comes to business-oriented backgrounds.

**Question 1:** In response to the first question, 76 respondents, or 48.7% of the total, strongly agreed with the statement; 78 respondents, or 50% of the total, essentially agreed; and, last but not least, just 2 respondents, or 1.3% of the total, had strong disagreements with the statement. While 1.3% of respondents "strongly disagreed" that management should be responsible for ensuring that a business is secured against Cybercrime, none of the participants essentially "disagreed."

According to the compiled summary of replies, this only means that out of all respondents, 154 respondents had the greatest count of frequency for those who agreed (SA & A) and were receptive to the truth.

**Question 2**: In response to this question, 6 responders in total highly agreed with the question. (With a percentage of 3.8%), 6 respondents who somewhat agreed with the question (with a valid percentage of 3.8%), 110 respondents who disagreed (70.5%), and 34 out of 156 respondents who severely disagreed (21.8%).

This only illustrates that, based on the replies, only 12 people agreed or strongly agreed with the statement.

**Question 3**: The related question on employees' attitudes regarding Cybersecurity in the workplace was posed here. After responding, respondents were once again categorized based on how strongly they agreed, disagreed, strongly disagreed, and agree. 43 respondents, or 276.6% of the sample, strongly agreed with the statement; 104 respondents, or 66.7% of the sample, essentially "agreed"; 6 respondents, or 3.8% of the sample, disagreed; and 3 more respondents, or roughly 1.9% of the sample, strongly disagreed.

Thus, it is clear from all of the responses to the third question that, taken together, a maximum of 147 responses expressed agreement or strong agreement with the statement that each member of the establishment is essential to defending the organization from criminal threats.

**Question 4**: 20 respondents, or 12.8% of the total, highly agreed with the fourth question; 109 respondents, or 69.9% of the respondents, agreed with the question in general; 21 respondents, or workers, disagreed with the question in 13.5% of the responses; and around 6 out of 156 respondents, or 3.8% of the respondents, severely disagreed.

Using the assembled summary of answers, it can be inferred that among those who responded, the most frequency count of responders who Agreed and Strongly Agreed was 129. indicating that they acknowledged the difficulty of knowing how they could help protect the company from Cybercrimes.

**Question 5**: In reference to this question, the responses obtained showed that, out of the total respondents, 21 respondents (or 13.5%) strongly agreed with the fact; 106 respondents (or 67.9%) essentially concurred when prompted; Of those surveyed, 14 (or 4.5%) strongly disagreed regarding the fact, whereas 23 (or 14.7%) disagreed just some extent.

Therefore, based on the overall number of replies, it may be inferred that the greatest frequency count of respondents who essentially and firmly agreed with the fact was 127. We obtained a total of 127 out of 156 potential responses by essentially summarizing the respondents who agreed and strongly agreed.

**Question 6**: Those with some experience working for the companies/organizations that they are employed were asked if they felt that IT security is a priority in the workplace.

12 respondents, or 7.7% of the overall, strongly agreed with the statement out of a possible 156. While 61 respondents, or 39.1%, chose to disagree, 36 respondents, or 23.1%, essentially agreed. Lastly, 30.1% of the 156 responders, or 47 people, "strongly disagreed."

Put another way, upon reviewing the compiled responses, it was evident once more that the idea that an organization's information privacy is its top priority received favorable feedback. This was evidenced by the respondents who disagreed, who had the largest frequency count (61), In spite of the fact that a total of 48 out of 156 Respondents concurred with the statement, often strongly concurring.

**Question 7**: In response to the question "Do computers offer all the protection a company wants?", there were 24 valid responses, or 15.4% of the respondents, who strongly agreed. Another 88 respondents, or 56.4% of the respondents, essentially agreed to the assertion, 35 responders, or 22.4% disagreed, as well as 9 more responders, or roughly 5.8% of the possible 156 respondents, strongly disagreed.

This just shows that, out of all the respondents, the greatest frequency count was 112, which represented the combined opinion of those who agreed and strongly agreed to the assertion.

**Question 8**: A number of people who have been collaborating with the aforementioned firms in relation to this study have once again responded to the subject of whether reporting Cybercrime is a waste of time. 8 of the 156 respondents or 5.1 percent of the sample strongly agreed with the statement; 51 more respondents or 32.7% of the sample basically agreed; however, 67 respondents or 42.9% of the sample blatantly disagreed with the question; and 30 more respondents or 19.2% of the sample strongly disagreed.

As a result, it is clear from all of the responses to the eighth question that the combination of respondents who disagreed or strongly disagreed with the statement that it is a waste of time to report a Cybercrime was, at most, 97 candid responses.

**Question 9**: this question was included in the questionnaires for the responders, and once more, the answers were divided into the divisions that had been previously mentioned. Regarding this specific question, a total of 39 respondents having a valid percent of 25.0% strongly agreed, followed by 102 respondents having a valid percent of 65.4% who essentially agreed with the question, 7 respondents having a valid percent

of 4.5% disagreed, and 8 out of 156 respondents having a valid percent of 5.1% strongly disagreed.

Based on the compiled summary of replies, it can be inferred that out of all respondents, 141 respondents had the highest frequency count of agreeing (Strongly Agreed & Agreed) and were receptive to the fact.

**Question 10**: The tenth question was one that was only included in the questionnaire and was equally important. For this specific question, the valid percentage of respondents who strongly agreed with the question was 26.9%, followed by 101 respondents who basically agreed with the question (64.7%), 9 respondents who disagreed (5.8%), and 4 respondents (2.6%) out of 156 respondents who strongly disagreed with the statement that cybercriminals are more advanced than the people who are supposed to be protecting us.

Based on the compiled summary of replies, it can be inferred that out of all respondents, 143 respondents had the highest frequency count of agreeing (Strongly Agreed & Agreed) and were receptive to the fact.

**Question 11**: This particular question was included to the survey, and the results were obtained. About 18 respondents, or 11.5% of the total, strongly agreed with the statement; 120 respondents, or 76.9%, essentially agreed; 17 respondents, or 10.9%, disagreed; and, finally, one more respondent, or 1 out of 156, who had essentially 0.6% strongly disagreed with the question, expressed concern about it.

After collation, this only shows that, of the replies, the greatest frequency count was 138 respondents, all of whom agreed and strongly agreed that reporting a cyberattack to the authorities would harm the company's reputation.

**Question 12**: for this question, 10 respondents with a valid percentage of 6.4% strongly agreed with the question; 6 respondents with a valid percentage of 3.8% essentially agreed with the question; 118 respondents with a total percentage of 75.6% disagreed with the statement; and 22 respondents with a valid percentage of 14.1% strongly disagreed with the fact stated.

According to the summary of collected replies, it can be inferred that out of all respondents, 118 workers disagreed with the statement at the highest frequency, while a total of 140 respondents disagreed and strongly disagreed.

**Question 13**: Only 1 respondent out of 156 with a valid percentage of 0.6% strongly agreed that they are aware of the company's IT policy and make an effort to follow it; 15 respondents with a valid value of 9.6% essentially agreed with the statement; 122 respondents with a valid value of 78.2% disagreed; and 18 more respondents with a valid value of 11.5 percent strongly disagreed with the statement.

Stated differently, the analysis of the compiled replies revealed that the respondents were not in favor of the notion that employees should be aware of the company's IT policy before attempting to utilize it. There were 140 strong disagreements and disagreements with the statement overall among the replies.

**Question 14**: Regarding the question of whether the network is protected from hacking and tampering with information, another questionnaire question had roughly 19 respondents with a valid percentage of 12.2% strongly agreed, followed by 115 respondents with 73.7% basically agreeing with the statement, 16 of these respondents with 10.3 percent virtually disagreeing, and finally, another 6 out of 156 respondents with essentially 3.8% strongly disagreed.

After collation, this only shows that, according to the replies, 134 respondents had the greatest frequency count, and they all agreed—and strongly agreed—that they would not know how to report a cyberattack if one happened.

**Question 15**: This assertion was yet another crucial query that was only included in the survey. In particular, 12 respondents with a valid percentage of 7.7% strongly agreed with the question; 85 respondents with a valid percentage of 54.5% basically agreed with the question; 43 respondents with a valid percentage of 27.6% disagreed; and, last but not least, 16 respondents out of 156 strongly disagreed with the fact.

According to the summary of responses compiled, it can be concluded that, among those who responded, the greatest frequency count for those who agreed (Strongly Agreed & Agreed) was 97. These respondents acknowledged that, in general, they wouldn't know for sure that they were required to report a cyber-attack in the establishment.

**Question 16**: Another crucial question in the questionnaire had answers obtained regarding this: 14 respondents, or 8.0% of the total, strongly agreed with the statement; 47.4% of the respondents, or 74, basically agreed when asked; 31.4% of the

respondents, or 49, simply disagreed with that fact; and 12.2% of the respondents, or 19 of them, strongly disagreed.

As a result, based on the total number of replies, it can be concluded that the greatest frequency count of respondents who essentially and really agreed with the truth was 88. We ended up with 88 replies out of a total of 156 since the respondents who agreed and strongly agreed were essentially combined.

**Question 17**: One of the questions posed to those with some knowledge of the aforementioned companies was, "I am confident that I will be able to spot the warning signs of a cyber-attack." Of the 156 respondents who could have responded, 11 of them (7.1%) strongly agreed that they would be able to recognize the warning signs of a cyberattack; 39 respondents (25.0%) essentially agreed with the statement; 98 respondents (62.8%) disagreed; and, last but not least, 8 respondents (5.1%) strongly disagreed.

Put another way, upon reviewing the compiled responses, it became evident once more that there were responses to the question of being able to recognize the warning signs of a cyberattack. Specifically, the number of respondents who disagreed or strongly disagreed with the statement up to 106 out of 156 could be considered.

**Question 18**: Several people who have been working with the civil registration were responding to this question once more. Of the 156 respondents who could have responded, 9 respondents with a percentage of 5.8 strongly agreed, followed by 19 respondents with 12.2% who essentially "agreed" with the statement, 111 respondents with 71.2 percent who had to disagree, and finally, another 17 respondents with a percentage of basically 10.9% strongly disagreed.

Consequently, it is clear from all of the responses to the eighteenth question that, at most, 128 candid responses represented the combination of respondents who disagreed or strongly disagreed with the statement that they believe the primary risk to IT systems arises from people working for the organization.

**Question 19**: This is an additional question from the survey that was sent to the participants. About the same number of respondents (workers) agreed and strongly agreed, respectively. 6 respondents with a valid percentage of 3.8% strongly agreed with the statement, and 6 more respondents with a percentage of 3.8% agreed with it in

general. Now, 23 out of 156 respondents, or around 14.7%, strongly disagreed with that statement on the belief that anyone working for the establishment is vulnerable to manipulation by arrogant fraudsters, while 121 respondents, or 77.6%, had to disagree outright.

After collation, this only shows that, of the replies, the greatest frequency count was 144 respondents, all of whom rejected and strongly disagreed with the statement that anyone within the system is vulnerable to manipulation by arrogant con artists.

**Question 20**: Now, for those who choose to fill it out, this item was added back to the questionnaire. A total of 31 respondents gave a valid percentage of 19.9% to strongly agree with the question; 114 respondents gave a percentage of 69.5% to essentially agree with the issue; and 11 respondents gave a percentage of 7.1% to disagree. None of the aforementioned workers "strongly disagreed" with the assertion.

This only illustrates that, according to the replies, 145 respondents agreed and strongly agreed with the fact, which was the greatest frequency count.

**Question 21**: Once more, the purpose of this inquiry was to find out how the staff felt about Cybersecurity in the workplace. This was yet another crucial query that was only included in the survey. In particular, 27 respondents gave a valid percentage of 17.3% strongly agreeing with the question; 117 respondents gave a valid percentage of 75.0% basically agreeing with the question; 11 respondents gave a valid percentage of 7.1% disagreeing; and last but not least, 3 respondents out of 156 gave a valid percentage of 0.6% strongly disagreeing with the fact.

Based on the summary of responses compiled, it can be concluded that, among those who responded, the greatest frequency count for those who agreed (Strongly Agreed & Agreed) was 144. These respondents responded to the statement that they do, in fact, think that hackers and cybercriminals target only large companies.

**Question 22**: No, this was the last question on the questionnaire, but it wasn't the least important one. Out of 156 respondents, 9 strongly disagreed, 26 disagreed, and 21 respondents strongly agreed, accounting for 13.5% of the total. 99 respondents essentially agreed with the question, while 63.5% disagreed.

When all data are combined and summarized, it is evident that 112 (78.2%) of the 156 participants denied that they were unaware of the company's IT policy. A further 117

individuals, or 75%, concurred that hackers exclusively target large organizations. However, 109 participants, or 69.9%, stated they were unsure of the best ways to defend the company from Cybercrimes and assaults. Stated differently, they consented to that.

Now, 2 lowest values were obtained from the collated data, as opposed to obtaining the biggest numbers of participants who agreed or disagreed with certain issues. Out of 156 participants, only 1 (0.6%) thought that hackers and cybercriminals target large firms. Additionally, 1 participant (0.6%) strongly disagreed with the statement that they were concerned about harming the company's reputation while or after reporting a Cybercrime or attack to the authorities.

## 4.5 Analysis of the Result and Hypothesis Testing

Analysis utilizing Pearson correlation was carried out to ascertain the correlation between variables (dependent and independent) in order to assess the validity of the hypothesis. The independent factors include age, gender, position at work, and experience, whereas the dependent variable is based on the "attitude towards Cybersecurity in business (ATC-IB)". The coefficient of correlation is denoted by the letter "cc". We would now test two hypotheses, one of which held the alternative hypothesis and the other the null hypothesis. Therefore, if the significant value is almost less than 0.05, it indicates that the alternative hypothesis should be accepted and the hypothesis with the null properties should be rejected. Essentially, "P<0.05".

### 4.5.1 Employees' age on attitude towards Cybercrime/Cybersecurity

For the first hypothesis, the "Pearson's correlation" approach would be used to analyze the relationship between the age of the employees and their attitudes on Cybersecurity and Cybercrime.

H1: There is a significant correlation between employees' age and their attitude towards Cybersecurity or Cybercrime

H0: There is no significant correlation between employees' age and their attitude towards Cybersecurity or Cybercrime.

**Table 4.5:** Pearson's correlation (employees' age and attitude towards Cybercrime/Cybersecurity in business)

| Correlations | | | |
|---|---|---|---|
| | | **ATC-IB** | **Age** |
| Age | Pearson Correlation | 1 | .830** |
| | Sig. (2-tailed) | | .001 |
| | N | 156 | 156 |

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

Table 4.5 illustrates the computation used to more precisely assess the correlation between the age of employees and their perceptions of Cybersecurity and Cybercrime in business (ATC-IB). The same Table (Table 4.5) makes it evident that the two variables (employees' age and ATC-IB) have a somewhat positive correlation (cc =.830, N = 156, P =.001). Now, this study unequivocally shows that the two variables the employees' age and their ATC-IB, respectively have a positive association, with a value that is rather near to 1. Furthermore, Sig. 2-tailed suggests that the two variables have a strong association. Thus, the hypothesis's H1 will be selected and accepted.

A similar study by Neiss [61] also proposed the difference in attitude and perception to Cybercrime among different age groups. They further stated that the difference is as a result of dissimilarities in perspective between young people and old age group. Younger people are driven by their emotional perception which is different from the older adults.

### 4.5.2 Employees' gender on attitude towards Cybercrime/Cybersecurity

For the second hypothesis, the "independent t-test" approach will be used to analyze the relationship between the employees' gender and their attitudes on Cybersecurity and Cybercrime for the next hypothesis.

H2: There is a significant correlation between employees' gender and their attitude towards Cybersecurity or Cybercrime.

H0: There is no significant correlation between employees' gender and their attitude towards Cybersecurity or Cybercrime.

**Table 4.6**: Statistical difference between employees' gender and attitude towards Cybercrime/Cybersecurity (Independent t-test)

| Gender | N | Mean | SD | Mean Difference | t | P |
|---|---|---|---|---|---|---|
| Male | 92 | 2.347 | 0.58 | .001 | .008 | 0.947 |
| Female | 64 | 2.346 | 0.57 | | | |

As can be seen in Table 4.6, the independent t-test was employed to examine the association between each employee's gender and their overall ATC-IB in order to demonstrate consistency. To put it another way, the researcher tested each dimension of the previously stated primary hypothesis using an independent t-test to see whether or not it satisfied each parametric test. With reference to Table 4.6 above, the results obtained indicate that, inasmuch as the number of male counterparts is greater than that of female counterparts, there is no significant difference between the two variables (t =.008, p = 0.947) in the outputs for men (M = 2.347, SD = 0.58) and females (M = 2.346, SD = 0.57). Once again, these unambiguous findings demonstrate that attitudes on Cybersecurity in work-related contexts do not change significantly based on a person's gender. Additionally, Sig. 2-tailed suggests that the two variables (each employee's gender and attitude toward Cybersecurity in business, or ATC-IB) do not significantly correlate.

Contrarily, study by Hasanet [62] suggested that there are differences in how men and women see Cybersecurity and that, in comparison to men, women are more conscious of online rules and adhere to online ethical standards. Previous literary analyses have demonstrated that differences in life styles are often linked to the demographic background of a person's sex group. Accordingly, when compared to those researchers' earlier study, the male participant in this one has a more positive attitude about Cybersecurity in the workplace than do the female equivalents

### 4.5.3 Employees' position at work on attitude towards Cybercrime/Cybersecurity

For the third hypothesis, ANOVA is used in this section to analyze the relationship between the variables presented. The goal of the research is to determine whether there is a relationship of any significance between the employees' attitudes regarding

Cybersecurity in business (ATC-IB) and their positions at work (Manager, Supervisor, Senior Laborer, and Junior Laborer).

H3: There is relevant impact that exists between Employees' position at work and attitude towards Cybercrime/Cybersecurity.

H0: There is no relevant impact that exists between Employees' position at work and attitude towards Cybercrime/Cybersecurity.

**Table 4.7:** One-way ANOVA on the impact of the position at work towards the attitude of Cybercrime and Cybersecurity in business.

| | Position | N | Mean | SD | F | Sig. |
|---|---|---|---|---|---|---|
| ATC-IB | Manager | 26 | 1.44 | 0.323 | | |
| | Supervisor | 83 | 2.28 | 0.145 | | |
| | Senior laborer | 40 | 2.83 | 0.317 | 262.898 | 0.001 |
| | Junior laborer | 7 | 0.70 | 0.185 | | |
| | Total | 156 | 2.34 | 0.582 | | |

*The mean difference is significant at .05 level

The influence of job positions on ATC-IB has been examined and tabulated from Table 4.7, and the results have been utilized to examine any discrepancies between two or more means. An investigation on the potential influence of a position on attitudes towards Cybercrime and Cybersecurity was carried out using a one-way ANOVA between groups analysis of variance. Based on their various positions, the employees (participants) were divided into four groups: Manager, Supervisor, Senior Laborer, and Junior Laborer. ANOVA statistics showed that there was a statistically significant difference between position and attitude toward cyber-crime and cyber-security ($F = 262.898$, $p = .001$; indicating that $p < .05$).

Table 4.7 clearly shows that the mean score for Manager was (M=1.44, SD=0.323), for Supervisor it was (M=2.28, SD=0.145), for Senior Laborer it was (M=2.83, SD=0.317), and for Junior Laborer it was (M=0.70, SD=0.185) according to post hoc comparisons using the Tukey HSD test. According to the data, customers who hold the Senior laborer job had the highest mean score (2.83) in the area of general attitudes concerning Cybersecurity and Cybercrime compared to the other customers. As a result, the

alternative hypothesis (H3), which claims that an employee's position at work has a relevant influence on their ATC-IB, is accepted.

According to a researcher and his team, one important finding from the investigation on employees' attitudes is that it demonstrates their apparent understanding of decentralized responsibility with regard to duties regarding Cybersecurity in a business. This fits theoretically with suggestions made by Tischer [63] that organizations are giving methodological mediators and senior management responsibility for their Cybersecurity. It appears that the strategy is for them to stop viewing Cybersecurity as their biggest worry as soon as they return to official work, especially if they hold higher positions. This would also fit well into a risk-benefit paradigm, in which some individuals who believe the technological assistance provided by their main employer will keep them safe may choose to engage in riskier Cybersecurity activities [17].

Thus, it is evident from the study's findings that employment roles have an effect on how businesses view Cybersecurity in the modern workplace.

### 4.5.4 Employees' experience on attitude towards Cybercrime/Cybersecurity

for the last hypothesis, the "one-way ANOVA" approach will be used to analyze the relationship between the employees' experience and their attitudes on Cybersecurity and Cybercrime for the following hypothesis. This would determine whether these workers' experiences may have an impact on how businesses view Cybersecurity.

H4: There is relevant impact that exists between Experience at work and attitude towards Cybercrime/Cybersecurity.

H0: There is no relevant impact that exists between Experience and attitude towards Cybercrime/Cybersecurity.

**Table 4:8:** One-way ANOVA on the impact of the experience towards the attitude of Cybercrime and Cybersecurity in business.

| | Years of experience | N | Mean (M) | SD | F | Sig. |
|---|---|---|---|---|---|---|
| ATC-IB | Less than 5 years | 41 | 1.65 | 0.385 | | |
| | 5-10 years | 43 | 2.28 | 0.067 | | |
| | 10-15 years | 15 | 2.40 | 0.029 | 106.870 | 0.01 |
| | Above 15 years | 57 | 2.87 | 0.439 | | |
| | Total | 156 | 2.34 | 0.582 | | |

*The mean difference is significant at .05 level

A one-way Analysis of Variance (ANOVA) among the groups was carried out in Table 4.8 to investigate the potential impact of experience years on attitudes on Cybercrime and Cybersecurity. Depending on how long they had worked for the company, the participants were split into four groups: under five years, five to ten years, ten to fifteen years, and more than fifteen years. Their differences using ANOVA statistics were statistically significant ($F = 106.870$, $p = 0.001$, indicating that $p < .05$), as Table 4.5 demonstrates. The mean score for workers with less than five years of experience is ($M=1.65$, $SD=0.385$), for those with five to ten years of experience, ($M=2.28$, $SD=0.067$), for those with ten to fifteen years of experience, ($M=2.40$, $SD=0.029$), and finally, ($M=2.87$, $SD=0.439$). These Post hoc contrasts were again determined using the Turkey HSD test. According to the data, workers who have been there for 15 years or more had the highest mean score (2.87) in the category of general attitudes regarding Cybersecurity and Cybercrime compared to the other workers.

As a result, the alternative hypothesis (H4), according to which employee experience has significant impact on the ATC-IB, is accepted.

### 4.6 Summary of the Hypothesis Test

Following this, the hypothesis was subjected to a "non-parametric" test, and Table 4.4 clearly shows whether the null hypothesis was accepted or rejected and whether the same ideology was applied for the alternative hypothesis. These Tables pertain to the Employees' ATC-IB with respect to Age, Gender, and Their Various Positions at Work.

**Table 4.9:** Summary of the Hypothesis Test

| Hypothesis | Verdict |
|---|---|
| $H1_1$: There is a significant correlation between employees' age and their attitude towards Cybersecurity or Cybercrime. | Alternate hypothesis = Accepted<br>Null hypothesis = Rejected |
| $H2_0$: There is no significant correlation between employees' gender and their attitude towards Cybersecurity or Cybercrime | Alternate hypothesis = Rejected<br>Null hypothesis = Accepted |

| | |
|---|---|
| $H3_1$: There is a significant correlation between employees' position at work and their attitude towards Cybersecurity or Cybercrime. | Alternate hypothesis = Accepted<br>Null hypothesis = Rejected |
| $H4_1$ There is a significant correlation between employees' Experience and their attitude toward Cybersecurity or Cybercrime. | Alternate hypothesis = Accepted<br>Null hypothesis = Rejected |

---

In addition, Figure 4.1 provides a clear illustration of the block diagram summarizing the preceding hypothesis results regarding the dependent variable (ATC-IB) and the independent variables (age, gender, position at work, and experience).

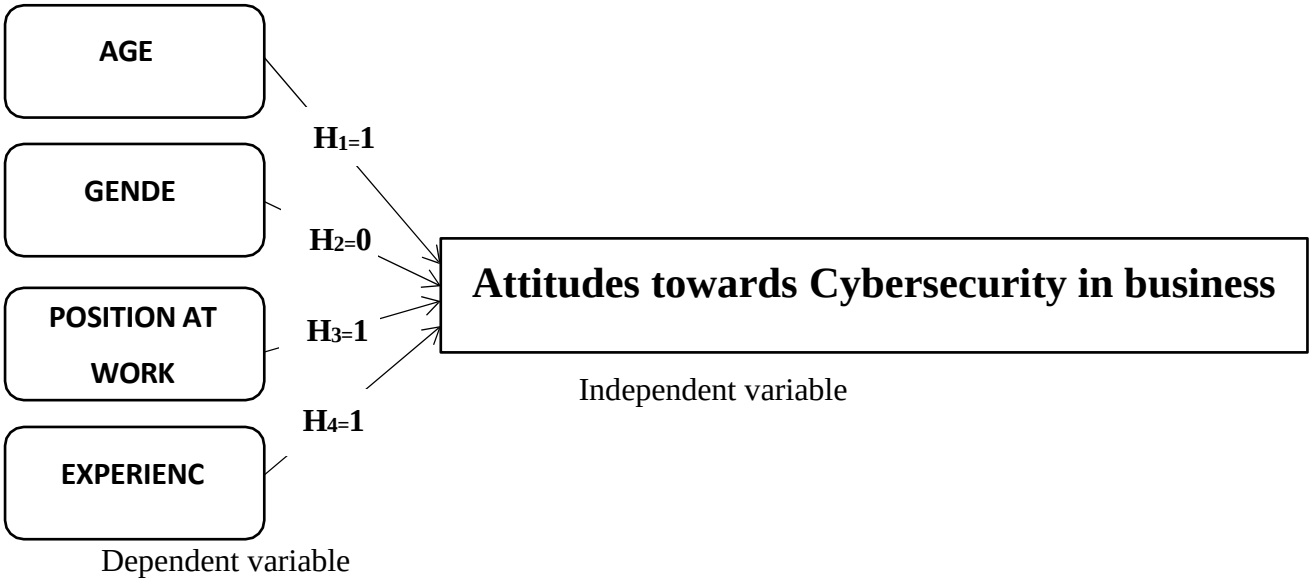



**Figure 4:6** Summary of the hypothesis result in block diagram

Taking a look at Figure 4.6, it is clear that the alternate hypothesis, which was accepted, was associated with the beta value for the age frame used in the attitude toward Cybercrime/Cybersecurity in business, "H1: 0. 830." This indicates that there was a positive significance, indicating that employees were completely satisfied with the effect of ATC-IB on the ages of the employees in certain organizations.

Gender, the dependent variable linked to the accepted null hypothesis, indicates little to no relevance. Employees' perceptions of the ATB-IC about their gender were therefore unfavorable.

This time, the dependent variable position of work indicates that the significance was sufficiently positive, which leads to the conclusion that employees were once again highly satisfied with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB) in relation to their various positions. As a result, the alternative hypothesis was accepted.

Last but not least, the ANOVA analysis of the final dependent variable experience reveals that the significance was positive enough, which leads to the conclusion that the employees were again highly satisfied with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB) based on their varied experiences, particularly when they have more experience working for a company.

# Chapter 5
# CONCLUSION AND RECOMMENDATION

## 5.1 Introduction

This chapter offers a succinct summary of the interview results. As stated in the section on research methods, the quantitative nature of this study necessitates an investigation that repetitively analyzes participant data to identify corresponding patterns. The headings are determined by the similarity of the participants' responses. By using the same terminology as the participants, the presented results eliminate the possibility of biased data. The thesis will now begin mapping and comparing these values, as it has now completed the necessary procedures for locating the appropriate data values for this research.

## 5.2 Recommendations

Following a battery of tests, analyses, and verifications for this study, it was discovered that most respondents tended to simply "agree" on the provided questions rather than "strongly agree" with regard to all four of the hypotheses that had to do with the employees' "age," "gender," "position at work," and "experience," which in turn was attributed to their attitude toward Cybersecurity in business. This could be because they were not fully aware of or satisfied with the general attitude regarding Cybersecurity in business. Therefore, it is recommended that modern technology be introduced and some attitudes related to it be created in Somalia's workplaces in order to improve employees' perceptions of Cybersecurity in today's businesses. This would undoubtedly have an impact on the high caliber of work produced in our workplaces. If there are existing ones in place at work, they ought to be strengthened even more to increase the likelihood of informing staff members that meeting their needs is crucial and should not be compromised.

## 5.3 Future Study

Once more, the researcher of this study has determined that it is appropriate to recommend that additional research be conducted in additional Somalian cities in order to practically analyze and determine the impact of any attribute related to the attitude of Cybersecurity in businesses (ATC-IB). This is after verifying the results obtained in this research.

## 5.4 Conclusion

Employees who answered the questionnaires intended for this study appeared to have a positive attitude about Cybercrime and security, as evidenced by the descriptive analysis, the Pearson correlation analysis, and the ANOVA thorough analysis. Additionally, each employee's gender essentially indicates that their male counterparts (with a descriptive analysis of 92) appreciated or participated in expressing their views on how they individually felt about Cybersecurity in today's diverse firms.

Furthermore, this study's research has demonstrated that, in fact, the opinions being expressed regarding Cybersecurity in the workplace are noteworthy in light of the effects it has on workers of all ages, genders, roles held within the company, and degrees of expertise.

In general, four hypotheses were put out; three of the alternative hypotheses were accepted, but only one of the null hypotheses was accepted. Thus, the study's goal was accomplished, which was to show that, generally speaking, attitudes about Cybersecurity in the workplace had a significant impact on employees' ages, positions held at work, and experiences with the exception of gender, which showed no impact and thus supported the null hypothesis.

With only three (3) dependent variables and one (1) dependent variable, it was observed that the alternate hypothesis, which was accepted, was associated with the beta value "H1: 0. 830" regarding the age frame applied to ATC-IB. This indicates that there was a positive significance, indicating that the age of the employees had a relevant impact on ATC-IB. Every employee who had to take time out to complete the questionnaire is essentially responsible for the age in question.

Furthermore, there is no positive significance for the dependent variable gender, which is linked to the acceptance of the null hypothesis. This basically means that every employee whose gender was revealed in the poll said that attitudes on Cybercrime and security in the workplace should not be kept positive. Based on the research findings, the gender of these employees had no impact on the output that was submitted to the ATC-IB.

This time, the dependent variable position of work indicates that the significance was sufficiently positive, which leads to the conclusion that employees were once again

extremely pleased with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB) in relation to their various positions. As a result, the alternative hypothesis was accepted.

Last but not least, the ANOVA analysis of the final dependent variable experience reveals that the significance was positive enough, which leads to the conclusion that the employees were again extremely pleased with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB) based on their varied experiences, particularly when they have more experience working for a company.

Therefore, the intended result, which demonstrates a very favorable significant influence in these related data, is as follows: the alternative was rejected and a null hypothesis was accepted, but the three hypotheses and their null were accepted. demonstrating that, with the exception of the workers' gender, which did not exhibit any positive attitude toward ATC-IB, the dependent variables (employees' age, experience, and position at work) depicted a connection that is fairly robust with regard to the Attitude towards Cybersecurity in Today's Businesses.

# References


[1] R. Deibert and R. Rohozinski, "Risking security: Policies and paradoxes of cyberspace security," *nternational Political Sociology*, vol. 4, no. 1, pp. 15-32, 2010.

[2] Z. Xuesong, F. Wang and Y. Ma, "An overview on energy internet.," in *IEEE International Conference on Mechatronics and Automation (ICMA)*, Beijing, 2015.

[3] C. Junwei and M. Yang, "Energy internet--towards smart grid 2.0," in *2013 Fourth International Conference on Networking and Distributed Computing*, Los Angeles, 2013.

[4] M. Wazid, S. Zeadally and A. Das, "Mobile banking: evolution and threats: malware threats and security solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56-60, 2019.

[5] S. Salsabeel, F. Qatan, R. Aburukba, F. Aloul and A. Ali, "Smart grid Cybersecurity: Challenges and solutions," in *International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, Offenburg, 2015.

[6] E. Göran, "Cybersecurity and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power delivery*, vol. 25, no. 3, pp. 1501-1507, 2010.

[7] C. Ta, C. Chen, C. Lee, C. Weng and C. Chen, "A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. Soft Computers," *Soft Computing*, vol. 22, pp. 2495-2506., 2018.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of network and computer applications*, vol. 34, no. 1, pp. 1-11, 011.

[9] J. Hamid, and A. Al-Nemrat, "Cybercrime profiling and trend analysis," in *Intelligence Management*, London, Intelligence Management: Knowledge Driven Frameworks for Combating Terrorism and Organized Crime, 2011, pp. 181-197.

[10] K. Wall, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang and J. Wu, "A survey on energy internet Architecture approach and emerging technologies," *IEEE systems journal*, vol. 12, no. 3, pp. 2403-2416, 2017.

[11] D. Matias and G. Mesch, "An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices," *Computers & Security*, vol. 86, pp. 75-91, 2019.

[12] B. Howe, "Commentary: Sir Bernard Hogan-Howe on new Cybercrime push," *The Standard*, 21 June 2019.

[13] z. Zibin, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," IEEE International Congress on Big Data (BigData Congress), Honolulu, 2017.

[14] M. Dheerendra, A. Das and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Systems with Applications*, vol. 41, no. 18, pp. 8129-8143, 2014.

[15] N. Huansheng, H. Liu and L. Yang, "Cyberentity security in the internet of things," *Computer*, vol. 46, no. 4, pp. 46-53, 2013.

[16] D. Charlette, K. Osei-Bryson and S. Samoilenko, "Exploring the impacts of intrinsic variables on security compliance efficiency using DEA and MARS," in *Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D*, Dar es Salaam, Springer International Publishing, 2019, pp. 751-762.

[17] H. Lee and K. Parsons, "Can cyberloafing and Internet addiction affect organizational information security," *Cyberpsychology, Behavior, and Social Networking*, vol. 20, no. 9, pp. 567-571, 2017.

[18] E. Ilker, A. Musa and R. Alkassim, "Comparison of convenience sampling and purposive sampling," *American journal of theoretical and applied statistics*, vol. 5, no. 1, pp. 1-4, 2016).

[19] A. Esharenana E and L. Akpojotor, "Students' Experience with Group Assignment in a Nigerian Library and Information Science School," *Information Impact: Journal of Information and Knowledge Management*, vol. 9, no. 3, pp. 132-139, 2018.

[20] A. Colin G and J. Burn, "A strategic framework for the management of ERP enabled e-business change," *European journal of operational research* , vol. 146, no. 2, pp. 374-387, 2003.

[21] H. Harry, "ICT in Education in Somalia," Survey 0f ICT And Education in Somalia, Mogadishu, 2007.

[22] S. Kemp, "DIGITAL 2020: SOMALIA," datareportal, Mugdishu, 2020.

[23] M. Noor, "Mohamed, Ali Noor. "ICTs and Regional Economic Integration: An Anticipatory Scenario for the Horn of Africa," *International Journal of African Development*, vol. 2, no. 2, p. 5, 2015.

[24] S. Jangirala, A. Das, N. Kumar and J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 942-956, 2018.

[25] P. Unwin , ICT4D: Information and Communication Technology for Developmen, Cambridge: Cambridge University Press, 2009.

[26] Immigration and Refugee Board of Canada, "Somalia: Prevalence of cell phones and Internet cafes in Mogadishu, including the ability to use cell phones for financial transfers.," Immigration and Refugee Board of Canada, Mogadishu, 2015.

[27] H. Lancaster, "Telecoms, Mobile and Broadband - Statistics and Analyses," BuddeComm, Mogadishu, 2018.

[28] Kaspersky, "Kaspersky Security Bulletin 2020. Statistics," Kaspersky, 2020.

[29] A. Devi, Cyber Crime and Cybersecurity, Detecting and Mitigating Robotic Cybersecurity Risks,, 2017.

[30] B. Roderic, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, vol. 29, no. 3, pp. 408-433, 2006.

[31] G. Iginio and N. Sambuli, "Cybersecurity and cyber resilience in East Africa," Center for International Governance Innovation and Chatham house , 2015.

[32] B. Lee and A. Berlin, Defensive security handbook: best practices for securing infrastructure, O'Reilly Media, Inc., 2017.

[33] P. D. Little, " Somalia: Economy Without State (Bloomington and Indianapolis," Southern University, Baton Rouge, 2003.

[34] Symantec, " Cyber Crime & Cybersecurity Trends In Africa.," The Global Forum on Cyber Expertise, 2016.

[35] H. Bashir, "CYBERSECURITY IN SOMALIA," *Asia e University AeU*, pp. 1-2, 2019.

[36] S. Nicole, "Somalia: Media law in the absence of a state," *International Journal of Media & Cultural Politics*, vol. 8, no. 2-3, pp. 159-174, 2012.

[37] K. Nir, Cybercrime and Cybersecurity in the global South, Basingstoke: Plagrave macmillan, 2013.

[38] K. Nir, "Cybercrime and Cybersecurity in Africa," *Kshetri, Nir. Cybercrime and Cybersecurity in Africa." Journal of Global Information Technology Management* , vol. 22, no. 2, pp. 77-81, 2019.

[39] M. Seck, "Tackling the challenges of cyber-security in Africa," United Nations Economic Commission for Africa Policy Brief, 2014.

[40] H. Tejaswini and H. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of information systems*, vol. 18, no. 2, pp. 106-125, 2009.

[41] R. Majed and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Computers & Security*, vol. 80, pp. 211-223, 2019.

[42] C. SeEun, J. Martins and I. Bernik, "Information security: Listening to the perspective of organisational insiders," *Journal of information science*, vol. 44, no. 6, pp. 752-767, 2018.

[43] H. Sadaf, D. Selvam and P. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," *Computers & Security*, vol. 87, p. 101594, 2019.

[44] I. Suleman, "Social and contextual taxonomy of Cybercrime: Socioeconomic theory of Nigerian cybercriminals," *International Journal of Law, Crime and Justice*, vol. 47, pp. 44-57, 2016.

[45] P. Tang and H. Rush, "The Cybercrime ecosystem: Online innovation in the shadows?," *echnological Forecasting and Social Change*, vol. 80, no. 3, pp. 541-555, 2013.

[46] P. Leedy, J. Ormrod and L. Johnson, "Practical research: Planning and design," *Journal of Applied Learning & Teaching*, vol. 1, no. 2, pp. 73-74, 2014.

[47] S. James, G. Gripsrud, U. Olsson and R. Silkose, Research methods and data analysis for business decisions, Springer International Publishing, 2021.

[48] G. Pervez, K. Grønhaug and R. Strange, Research methods in business studies. Cambridge University Press, Cambridge: Cambridge University Press, 2020.

[49] R. Kerry, "A user-friendly practical guide to preparing data for analysis. In P. M," in *Quantitative Research Methods in Consumer Psychology*, Routledge, 2018, pp. 326-375..

[50] S. Daniel, G. Stockemer and J. Glaeser, Quantitative methods for the social sciences, Cham, Switzerland: Springer International Publishing, 2019.

[51] A. Alinda, "Information security policy compliance: Systematic literature review," *Procedia Computer Science*, vol. 161, pp. 1216-1224, 2019.

[52] K. Alex, J. Nord, Z. Sandoval and J. Paliszkiewicz, "Reliability, validity, and strength of a unified model for information security policy compliance," *Journal of Computer Information Systems* , vol. 61, no. 2, pp. 99-107, 2021.

[53] M. Gregory, M. Siponen and S. Pahnila, "Toward a unified model of information security policy compliance," *MIS quarterly,* vol. 42, no. 1, pp. 285-A22, 2018.

[54] D. Maslina,, R. Rasiah, M. George, D. Asirvatham and G. Thangiah, "Bridging the gap between organisational practices and Cybersecurity compliance: Can cooperation promote compliance in organisations," *International Journal of Business & Society,* vol. 19, no. 1, 2018.

[55] D. Maurice, "Applying a holistic Cybersecurity framework for global IT organizations.," *Business Information Review,* vol. 35, no. 2, pp. 60-67, 2018.

[56] J. Lennart, A. Eckhardt and A. Kroenung, "The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis.," *nformation & Management,* vol. 58, no. 3, p. 103318, 2021.

[57] O. Dustin, M. Warkentin and R. Crossler, "Integrating cognition with an affective lens to better understand information security policy compliance," *Journal of the Association for Information Systems* , vol. 20, no. 12, p. 4, 2019.

[58] H. Lee, "Human factors in Cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards Cybersecurity, and risky Cybersecurity behaviours.," *Heliyon,* vol. 3, no. 7, 2017.

[59] S. Mark, P. Lewis and A. Thornhill, "Research Methods for Business Students.," *Pearson education,* 2009.

[60] G. David and D. W. Straub, "Gender difference in the perception and use of e-mail: an extension to the technology acceptance model," *MIS quarterly,* pp. 389-400, 1997.

[61] N. Michelle , L. Leigland, N. Carlson and J. Janowsky, "Age differences in perception and awareness of emotion.," *Neurobiology of aging,* vol. 30, no. 8, pp. 1305-1313, 2009.

[62] H. Md Shamimul, R. Abdul Rahman, S. Abdillah and N. Omar, "Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia," *Journal of Social Sciences* , vol. 11, no. 4, p. 395, 2015.

[63] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein and M. Bailey, "Users Really Do Plug in USB Drives They Find," in *2016 IEEE Symposium on Security and Privacy (SP)*, an Jose, CA, USA, 2016.

# APPENDIX A
# QUESTIONNAIRE

**SECTION A:**

**Demographics of respondents**

1- What is your age?

(……)

Pleas indicate...

2- What is your gender?

◯Male

◯Female

3- what is your level level of education?

◯ high school

◯Bachelor

◯Master

◯PhD

4- position in organization?

◯Manager

◯senior labourer

◯Supervisor

◯ junior labourer

◯ Others ……

5- how long have you Worked at organization

◯less than 5 years

◯5 to 10 years

◯10 to 10 years

◯15 years and more

## SECTION: B

Please tick appropriately based on the level of your agreement

| NO | Scale items for the Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB). | **Strongly Agree** | **Agree** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 1 | I think that management have the responsibility to ensure a company is protected from Cybercrime | | | | |
| 2 | I am aware of my role in keeping the company protected from potential cybercriminals. | | | | |
| 3 | I believe everyone in the company has a role to play in protecting against threats from cybercriminals. | | | | |
| 4 | It is hard to know how I can help protect the organization from Cybercrime. | | | | |
| 5 | I don't have the right skills to be able to protect the organization from Cybercrime. | | | | |
| 6 | I do not feel that IT security is a priority within my organization. | | | | |
| 7 | Computer systems provide all the protection a company needs. | | | | |
| 8 | I think that reporting Cybercrime is a waste of time. | | | | |
| 9 | The Police lack the capacity to deal with Cybercrime effectively. | | | | |
| 10 | I believe that cybercriminals are more advanced than the people who are supposed to be protecting us. | | | | |
| 11 | I worry that if I report a cyber-attack to the Police, it might damage the reputation of the company | | | | |
| 12 | I think more could be done to communicate the risks from Cybercrime to individuals in the organization. | | | | |
| 13 | I am aware of the company's IT use policy and attempt to follow it. | | | | |
| 14 | I would not know how to report a cyber-attack if one happened. | | | | |
| 15 | I don't think that reporting a cyber-attack on the company is my responsibility. | | | | |
| 16 | I don’t pay attention to company material about the threats from Cybercrime. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 17 | I am confident that I would be able to spot the signs of a cyber-attack. | | | | |
| 18 | I think the biggest threat for IT systems comes from people within the company. | | | | |
| 19 | I feel that any individual within the company is at risk of manipulation from confidence tricksters. | | | | |
| 20 | I think that cybercriminals only target a company when there is a substantial financial gain. | | | | |
| 21 | I believe only large companies are targeted by hackers and cybercriminals. | | | | |
| 22 | I don't think I know who is responsible for protecting the company from Cybercrime. | | | | |