jamk.fi

Cybersecurity Awareness in Somalia

Survey in Public, Telecom companies, Bank and Government institutions

Abas Osman Nur

Master's thesis
April 2021
School of Technology, Communication and Transport
Degree Programme in Information and Communication Technology
Cybersecurity

jamk.fi

jamk.fi

Description

Author(s) Nur, Abas Osman	Type of publication Master's thesis	Date April 2021
	Number of pages 132	Language of publication: English
		Permission for web publication: Yes

Title of publication

Cybersecurity awareness in Somalia

Survey in Public, Telecom companies, Bank and Government Institutions

Degree programme

Master's Degree Program in Information Technology, Cyber Security

Supervisor(s)

Lappalainen-Kajan, Tarja; Hautamäki, Jari

Assigned by

-

Abstract

Cybersecurity awareness is a crucial component for maintaining a healthy cybersecurity state. Somalia is a developing nation with a fragile cybersecurity sector due to various issues, including lacking an official national cybersecurity strategy, an official functioning CERT (Computer Emergency Response Team), and national cybercrime regulations. Therefore, a critical evaluation of Somalia's cybersecurity state and awareness was studied.

The research investigated the level of cybersecurity awareness in Somalia, focusing on the general public, telecom service providers, banking and government institutions. The research was able to identify cybersecurity areas within these sectors with the highest knowledge gaps and thus provide insights into the different risk levels amongst the sectors.

A quantitative method in the form of a survey with the distribution of self-completion google forms was used to identify the level of cybersecurity awareness. The study had a total of 192 respondents across the four sectors. The principal method used during the study was a questionnaire survey which revealed how much the general public is aware of in terms of cybersecurity, what areas the banking and telecommunication sectors are lacking in, as well as what the government needs to do to improve the cybersecurity within the country as a whole.

An analysis of the survey results showed that Somalia has a weak cybersecurity state and low cybersecurity awareness level. Moreover, the research revealed that most participants have never received cybersecurity awareness training and thus were not prepared for the risks and threats from a pre-emptive perspective. The research is applicable in both the private and public sectors in Somalia since relevant stakeholders can exploit the results to mitigate existing challenges.

Keywords/tags (subjects)

Cybersecurity, research, survey analysis, banks, telecom, government, public awareness, Somalia

Contents

Figures

1 Introduction

At present, the African continent is more vulnerable to cyber threats than any other continent due to the lack of a cybersecurity framework or proper law (Kshetri, 2019). Although some countries are in the process of establishing their first cyber laws, cybercrimes are increasing at a drastic rate due to the increased attack surface that the internet provides to its users.

In Somalia, cybersecurity has become a national issue after the widespread global use of the Internet as many government operations and processes become digitalised. Cybercriminals use cyberspace to target the government's confidential assets to disrupt critical infrastructure, exfiltrate data, or steal citizens' personal information. These criminals targeting the Somali government's infrastructure have multiple motives, including, but not limited to, gaining financial benefits or providing intelligence information to adversaries (Sambuli et al., 2015).

Currently, Somalia lacks a national cybersecurity strategy and directives, including cybersecurity standards, frameworks, policies, and awareness programs. It is ranked as one of the worst cyber secure countries, indicating a massive gap between international standards and a national cybersecurity plan. It also lacks training and educational plans in regards to cybersecurity in the country. In particular, no platform where citizens can get an awareness of cybersecurity threats. This is since lack of knowledge is viewed as a factor that contributes to insecure online behaviour by internet users (Thomson et al., 2006). This is due to the fact that more effort is diverted towards incidents instead of focusing on prevention, which would in turn reduce the number of incidents received.

The fact that the thesis has no assignor goes to prove just how little thought goes into the cybersecurity field within Somalia, especially in terms of cybersecurity awareness, shadowing the ever more pressing need for this study. This highlights a research gap in Somalia and thus it is essential for Somalia to have a thorough understanding of the current level of cybersecurity awareness in order to implement relevant interventions.

In the current body of literature, there is only one published research that looks into cybersecurity awareness in Somalia, with its focus being on university students in Mogadishu (Warshaddaha, 2019). This focus on only university students which gives us a minuscule glimpse into the habits and behaviors of the people of Somalia in regard to cybersecurity. It does not provide data on the general public, workforce and the government, notwithstanding the fact that they are the ones mostly affected by cybercrime.

The study is expected to help guide the creation of cybersecurity awareness campaigns in Somalia by identifying key knowledge gaps within different critical infrastructure sectors. The research intends to answer the following questions:

1. What are the cybersecurity risks and threats, and their impacts?
2. What are the best practice approaches used by countries with successful cybersecurity awareness operations?
3. What is the current state of key Somalia sectors regarding cyber awareness and what areas of focus should be prioritised?

The research uses a mixed-methods approach drawing on both qualitative methods (document research in chapter 3, chapter 4, and chapter 5) and quantitative surveys (chapter 6). The qualitative documentary research utilizes both public and private documents to provide an overview of the risks, threats, and impacts of cybercrime.

The quantitative surveys focus specifically on Somalia and are completed online, therefore, the surveys are divided into four different sectors, namely: general public, telecommunications service providers, bank and government institutions. Each sector has a unique survey with best practices relevant questions to assess the current cybersecurity situation in the country.

2 Research

This research section describes concisely what the research seeks to achieve as well as the process by which this information was collected and analysed. By the end of the research, all objectives have to be achieved. Hence, this section acts as a guideline for the research.

2.1 Research Objectives

The goal of the thesis is to determine the current level of cybersecurity in Somalia, understand the main threats and impacts of cybercrime, and examine how private and public institutions counter them. This will be done by examining the level of implementation cybersecurity strategies and policies, both in private and public institutions. The main research objectives are:

- Identify cybercrimes and threats.
- Analyse the current cybersecurity awareness in Somalia.
- Recognize best practices from several successful countries as well as from less developed countries.
- Provide recommendations on cybersecurity areas to be selected in future awareness campaigns.

2.2 Qualitative and Quantitative Research Methods

There are two principal research methodologies used in this study: qualitative and quantitative methods. However, combining the two approaches creates a third approach, which is referred to as the mixed-method. The qualitative approach entails fieldwork whereby the researcher collects data using methods such as in-depth interviews, observation, focus groups and by reviewing the incumbent body of literature. The quantitative approach uses statistical analysis of data that is collected by querying individuals using questionnaires, polls, and surveys. This allows the data collected to be measurable and quantifiable.

The mixed-method approach combines quantitative and qualitative approaches, thus creating a neutral point for constructivism and positivism. The mixed approach

strives to address the criticism of each approach and facilitate the study by taking all-inclusive perspective. The main advantage of this method is that it cross-checks results using a variety of research methods (Krishnaswamy, 2016).

Considering the present-day situation of cybersecurity in Somalia: the lack of an established cybersecurity infrastructure, the qualitative method will help provide a base of information that will support the data collected and analysed from the quantitative methods. This will provide a holistic view of the situation within the country.

2.3 Data Collection and Data Analysis

The reliability and validity of the data research depends on the data collection model of the study (Krishnaswamy, 2016). This research will collect data from the following sources, namely, documentations and surveys.

The qualitative method will use data from the following sources namely, research papers, educational books, official websites, and other reputable online resources. Combining data from numerous sources increases the accuracy and dependability of qualitative data. The quantitative method will collect information by use of surveys. Getting participants for this study is hard; however, the study reveals that the data and information should be collected from senior ICT managers, IT professionals and general users.

Several data sources will be used in order to eliminate bias and to allow triangulation. The research study thus uses surveys to gather the data from targeted institutions and participants. The participants were not given prior knowledge of the questions in the survey in order to get original and genuine views on the various topics. Google Forms will be used to develop and distribute the surveys to the various participants. This ensures the data can be collected by various online methods like emails or the browser without the need to physically drop and pick up the forms. With the Covid-19 pandemic limiting movement and meetings, this method was selected to be the simplest and most efficient. Confidentiality and integrity of all the research data was maintained during the study. No data was

added or altered and the identities of the participants were kept off the record to protect their anonymity.

Responses to the surveys are neatly and automatically collected in Google Forms allowing instant analysis through charts and graphs. Inductive analysis was used to study the information collected by identifying patterns and relationships. This in turn allows us to create theories and recognize themes from the data. In inductive approach, the collected data needs to be analyzed and conclusions are made based on that (Saunders et al., 2009). This approach was chosen as few or no previous studies of the research question exist.

2.4 Making the Survey

A survey is a data collection model that uses structured questions to assess the perception of an individual about a given topic or concept. Hence, to avoid biases arising from using a single foundation of data, the study uses different surveys depending on the group of people being questioned. There were four distinct surveys created, one for each considered sector, that is, the general public, telecom service operators, banking and the government institutions.

The questions are simple, brief, and objective to avoid overload of data that may complicate the analysis. The participants answered the questions without any interference from the researcher and there was no attempt to convince the participants to adopt different viewpoints from those they originally held. Judiciously, the survey side-steps using too many open-ended questions, rather, it uses a closed-ended questioning style for easier evaluation of the data collected. These questions are easy to answer and create data that is easy to measure and as such, provide us with outright and complete answers.

The analysis of the survey always remained objective and there was no attempt to influence any participants towards a particular perspective or to select a specific choice. By providing a specific number of options to the questions, the statistical analysis of the collected data was straightforward, with a notable consistency of the responses noted.

2.5 Structure of the thesis

The thesis includes eight chapters. Chapter one comprises of the background, research questions and an overview of the study. Chapter two delivers the objectives of the study and the various methods by which the research was carried out. The third chapter presents a theoretical analysis, as well as related literatures, of the cyber risks and threats faced by society. The fourth chapter then dives into the ways different countries are solving the risks and threats mentioned in the chapter three above. The fifth chapter analyses the current state of cyber security within Somalia. Chapter six looks at the survey done across the four sectors and analyses the findings of the surveys. The seventh chapter describes the findings, and the eighty chapter is the final chapter and conclusion of the thesis.

3 Cyber Security Risks, Threats and Impact

3.1 Overview

The Internet is spreading precipitously in this era. The World Wide Web is now the important driver to access information, and this is possible because of abundant projects in computer networking that lead to producing communications protocols. With expansion of these protocols, cybersecurity is becoming more important to industries all over the world (Rouse, 2019). Organisations tend to have cyberspaces, and considering the dependency, security has become the mandatory feature. The parameters of cybersecurity are not only limited to robust network connections but also aligning of associate components, filtering, maintenance, and detection and prevention systems (Richard, 2019).

As such, cybersecurity has become a topic of global significance and intrigue. Effectively, more than 50 countries have developed, implemented, and distributed authoritative strategies and procedures outlining the official position in relation to various cybercrimes. Cybersecurity consists of the tools, rules and regulations, security ideas, best practices, innovations, and activities used to ensure the security of all digital activities. Today, the internet is integral to almost all life aspects, including communication, social interactions, mobile money and payment platforms,

and to establish and maintain businesses. An increased dependence on internet-enabled devices breeds new threats since they provide malicious hackers with increased motivations for committing cybercrimes. Cybersecurity risk is the probability of a loss, resulting from a cyberattack. A cyberattack is any attack within the cyberspace. Cyberthreats have a negative impact on individuals, businesses and governments. They are never static with loads being created every year. This risk is being compounded due to an increase in computers and mobile devices. The importance of recognising, classifying and communicating a cyberthreat is vital.

In this chapter, we analyse the concept of the Internet and the modern cyberspace in Somalia and examine the dependence on it. An analysis of information security then follows with a deep-dive into the CIA (Confidentiality, Integrity and Availability) triad. They were chosen as they serve as the basis of information security and usually work as guides for the protection of data. Data is then categorised in terms of sensitivity, as well as importance. We look at the following kinds of information: customer, product, employee and organisation, and how risk can be reduced in all the aforementioned areas. We then analyse cybercrimes, understanding the data and network crimes. Finally, we analyse the impacts of cybercrime by looking at the potential economic impacts, specifically the impact on businesses, employees, market value and customers. Understanding this impact can actually help create awareness and urgency to the need for cybersecurity.

3.2 Justification

The theory described in this section will be applied in developing the questionnaires to be used during the surveys and comprises the tenets of cybersecurity awareness and protection. Applying the theory in the survey will assist in assessing critical cybersecurity aspects and awareness in Somalia. In addition, the theory was chosen since it agrees with the quantitative research methodology adopted to facilitate the study. Evaluating multiple literature sources facilitates a factually-based theoretical basis for performing a study on the current cybersecurity awareness level and state in Somalia. Cybersecurity is a multidisciplinary field, and it is vital to understand cybersecurity components prior to formulating a research method for the study to be accurate and complete.

Understanding the cybersecurity risks, threats and impact is the most fitting way to create the required controls, policies, procedures, and practices for realizing more robust protection within the public and private sectors.

Furthermore, choosing the theory was informed by the fact that the essence and purpose of the study correlates to the chosen literature. The research aims to evaluate and analyse the current cybersecurity state in Somalia hence it is a prerogative to comprehend the theoretical aspects of cybersecurity processes and awareness. It is also pertinent to note that the literature review is developed based on numerous theoretical constructs. As such, a deep search on the internet and academic digital libraries was the primary criteria utilized to identify and select specific theoretical principles and concepts for meeting the objectives outlined in this study. The following sections provide detailed descriptions of various theories critical to the completion of the study.

3.3 Internet

The Internet is a global network that interconnects computer systems throughout the world for communication. The Internet transfers data from one computer to another regardless of their geographical location. To connect to the Internet, an Internet service provider (ISP) is mandatory, which performs the role of middleman between computer and the Internet (Woodford, 2020). The Internet has extended to 230 countries around the world in less than 20 years. Even some of the world's poorest developing nations are now connected. Today, the Internet is a public, cooperative, and self-sustaining that is accessible globally (Techterms, 2015).

Internet usage in Somalia began in the year 2000 and has grown steadily since then. However, the internet penetration rate remains low as only 2% of the population can access the internet (Woodford, 2020). Despite a low penetration rate, the below image show a rising trajectory over the years implying that more people connect to the internet today compared to previous years. The internet is the primary method for conducting cyberattacks, and with Somalia registering continuous growth, it is vital to evaluate the current cybersecurity state and awareness level in the country to determine how it can achieve stronger internet security.

3.3.1 Modern Cyberspace

Cyberspace is a concept that describes the environment of an interconnected digital network, and more exclusively, it is an electronic medium in which communication over the computer network occurs. Cyberspace engages users in multiple activities: it allows them to interact with each other, play games, carry out their business, and much more (Augenbaum, 2019). The term 'cyberspace' was initially introduced by William Gibson in his book *Neuromancer* in 1984 (Gibson, 1984). This term still widely refers to any feature or service that is available on the Internet.

In the 1990s, cyberspace was referred to as the location in which people interacted with each other while using the Internet. Many users in the early 1990s believed that cyberspace should not be bound to any rules or regulations by any national government (Bussell, 2013). With the emergence of different social websites and blogs in the early 21st century, cyberspace became so much more important in social and political discussions.

In the absence of a functioning government and state due to terrorism and other insecurity incidents, little has been done to secure the Somali cyberspace. According to Gagliardone & Sambuli (2015), the country has developed hybrid solutions that combine new technologies and traditional practices to enhance its cyberspace security, but the measures are largely inefficient. The current cyberthreat landscape comprises advanced and modern threats undetectable to most traditional security offerings.

Although Somalia combines both traditional methods and new technologies to protect itself from cyber-attacks, it is incapable of thwarting highly-motivated attacks, such as a state-sponsored attack. The government faces various hurdles in realizing robust national cybersecurity procedures. Therefore, an evaluation of the cybersecurity situation in Somalia by establishing factors inhibiting the government from realizing the desired cybersecurity state and awareness will go a long way in determining more proactive measures for protecting a modern cyberspace.

During the last two decades, the scope of the Internet and the dependency upon cyberspace for social, economic, governance and security functions has grown

rapidly. The access of unrestricted information through the Internet creates new debates on the privacy of individuals and governments. The governments and administrators of cyberspace started taking extreme measures to prevent the misuse of users' information (Menon, 2013). With growth in cyberspace comes new challenges within Somalia.

Gagliardone & Sambuli (2015) argues that although most Somali territories are synonymous with lawlessness and chaos stereotypes, reliance on cyberspace continues to increase. For example, telecommunications companies, radio stations, and mobile money companies depend on a secure cyberspace to provide Somalis with critical services. Furthermore, the country has made significant strides in fighting terror and related insecurities in recent years and has achieved better stability. The economy is slowly reopening with numerous enterprises springing up.

As such, it is a clear indication that the internet penetration rate will rise in the coming years. The government and all stakeholders require to understand the current cybersecurity state and awareness level in the country to make informed decisions regarding national cybersecurity protection for both private and public sectors. Therefore, a study evaluating the cybersecurity state in the private and public entities is critical to realizing a secure cyberspace that provides a lifeline to many entrepreneurs in an under-developed country.

3.4 Information Security

The term 'information security', also known as InfoSec, is the procedures and tools deployed to protect sensitive information from modification, destruction, inspection, and disruption. Information security is about protecting crucial information from unauthorised access, use, disclosure, disruption, modification, inspection or destruction. This confidential data may contain personal details, mobile phone data, biometrics, social media profiles, etc. (Cisco, 2020). If a security breach happens, infosec engineers are supposed to probe the cause and make efforts to reduce the impact of the incident. The main consideration of the professionals is to safeguard the confidentiality, integrity, and availability of information along with sustaining organisational productivity. This has encouraged professionals in the InfoSec industry

to create and enforce proper rules and regulations. These may include guidance, proper structuring of policies, setting standards on passwords, anti-malware, intrusion detection and prevention systems, and encryption software (Tunggal, 2020).

Information security and cybersecurity are often used interchangeably, however information security is a part of cybersecurity that focuses specifically on the security of information and data. That said, the survey questionnaires to be used in this study will be based on the basic principles of information security, which are confidentiality, integrity, and availability, to assess and evaluate the cybersecurity measures and awareness level of the country in relation to protecting valuable information. All cybersecurity processes must ascertain the availability of critical IT assets to ensure continued operations and access to vital data. Besides, with many users having access to essential systems, it is vital to develop and enforce policies governing accessibility as a measure of preserving system and data confidentiality. Applying the three information security concepts in the research will assist identify missing controls and strategies required to preserve availability, confidentially, and integrity.

3.4.1 Basic principles of information security

Information security is made up of three fundamental principles and they are: confidentiality, integrity and availability. To achieve an ideal outcome, every component of an information security programme should be designed to execute these three principles effectively (Burnette, 2020). During the research, we shall attempt to establish whether the information security procedures, and cybersecurity strategies in extension, are designed and implemented based on the following principles:

Confidentiality

This means that the data is unavailable to non-legitimate users and processes. The main theme of the confidentiality principle is to ensure that a user's personal data is secure and is only accessible by a legitimate person. Information confidentiality means ascertaining only users with the required access levels can access and use

sensitive information. Examples of cybersecurity measures for maintaining data confidentiality that will be part of the research include protection from password theft, laptop or mobile phone theft, and other security management techniques (Michael, 2011).

The confidentiality principle is vital to identifying relevant measures and controls for preventing unauthorized access instances. Insufficient access controls can permit anyone to access sensitive records, such as health information and customer personal information, exposing to theft risks. Researching on information and system confidentiality literatures will have a profound effect in the survey design as it is a basis for evaluating awareness and security protections for preventing unauthorized access in Somalia.

Integrity

The implementation of integrity ensures the accuracy, validity and completeness of data. This means it protects data from unauthorised modifications (e.g., add, delete or change). An organization must maintain data in its original state without attempted changes, modifications, or deletions to preserve its integrity. For instance, the data of an employee who has left their job within an organisation should be updated with a status of 'Job left'. This modification to the data should be done by an authorised person and no other person should be permitted to edit it (Angraini, 2019).

Preserving data and system integrity promotes reliable cybersecurity since it requires the adoption of policies and procedures governing access and use of critical assets. A user with access to customer data should only be permitted to use and modify it as per the granted access and usage permissions. Improper modification of data could result in inaccurate or incomplete outcomes, whereas compromising system integrity by making unauthorized settings or configurations could expose it to numerous cyber threats.

The surveys targeting the private and public organizations in Somalia will, therefore, evaluate their preparedness in preserving data and system integrity by assessing specific cybersecurity controls.

Availability

Availability ensures the availability of information on demand. Its purpose is to make data available anytime when needed. Today, a business cannot survive if the organisation has failed to provide data at any time. It makes information security professionals more concerned with ensuring availability by preventing power outages, hardware failure and denial of service attacks. Availability is considered as the basic fragment of an effective data security programme as inevitably it is the end-clients who should have the option to utilise the data (Michael, 2011).

On the same note, IT systems must be available round the clock to ensure business continuity. System availability implies having reliable technology solutions and backup alternatives in case the implemented ones fail. Some of the basic availability practices to be considered when researching the current cybersecurity awareness in Somalia include information and system backup operations.

System backup practices require an organization to make a backup of system configurations consistently such that they can be restored easily if new IT infrastructure is required as a result of an adversarial incident. Information backup operations are the measures taken to store information securely and defining the restoration procedures if a cyber-incident renders the current data unavailable.

3.4.2 Types of data that need to be secure

Data can be categorised according to its type, sensitivity and importance to the organisation. With the classification of data, an organisation considers the importance of the data, determines if the data at risk is of high value, and executes necessary controls to minimise the identified risks. There are several ways of categorising data according to its type, such as data at rest and data in motion. Data can also be classified based upon its level of sensitivity.

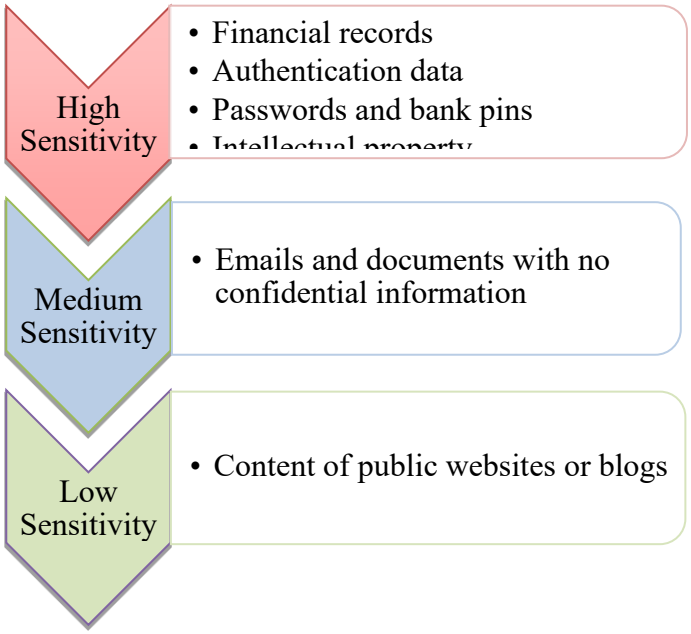
Categorizing data according to the sensitivity levels informs the required protection level. It is an efficient method of applying cybersecurity controls according to the data being protected since some types of information require higher security. As the

following sections will show, data with higher sensitivity needs more robust protection measures (Abhishek et al., 2015). Besides, data classification enables an organization to focus protection measures on highly sensitive data, saving costs and resources for securing other essential resources. The three data sensitivity types are:

High sensitive data: if breached or demolished in a non-legitimate engagement, this would have an immense effect on the reputation of an organisation or an individual. Bank details, other financial records, credentials, etc, can be classified here. The more sensitive data is, the greater the repercussions if a cyberattack destroys it or leads to information theft. Also, the costs are greater since highly sensitive data is more valuable. As such, it is pertinent for organizations to determine the most sensitive data and apply strong controls, such as encryption and monitoring measures, to protect it completely.

Medium sensitive data: this is data for internal use within the organisation, but may not have a devastating impact in case of a breach of information such as emails, confidential documents, etc. Organizations rely on data used for internal reasons to drive daily operations and it should always be available. Therefore, the cybersecurity measures applied to protect medium sensitivity data must be capable of protecting against modern threats. On this note, it is essential for the research to establish the controls organizations use to protect and secure their internal data.

Low sensitive data: this is data planned purposely for public access and includes content such as social media posts and unrestricted website material. For this type of data, a breach would result in minimal impacts for the affected organization. In any case, it is intended for public viewing and use. However, it is vital to protect the channels used to communicate or post such information. For example, malicious individuals can use an organization’s social media profile to share disturbing content, which may destroy the company’s reputation.



The types of data that require security with respect to their sensitivity are as follows (Arnold, 2017):

Customer Information

These days, consumers are more connected by sharing more information than before. They research online about products and services, take benefits from these services and purchase online through their devices. All this data is captured and stored by their ISPs, applications or websites, mobile operators and device manufacturers (Wright, 2019). They use this data for selling purposes, or they may use it internally.

Additionally, organizations in all industries collect personal data to provide services. For example, organizations in the healthcare industry, such as insurance firms and hospitals, collect sensitive health data. Businesses collect and store credit card details when customers make an online purchase. Customer data contains highly sensitive information requiring strong security controls to preserve its integrity, confidentiality, and availability.

As such, organizations should classify customer information as highly sensitive data and implement adequate measures to protect it. It essential to research an awareness levels of users interacting with customer data to determine suitable measures for securing it.

Almost all clients publish their personal information with the business they trust. To achieve and sustain this trust is crucial for businesses. Most organisations have very specific privacy rules and practices to gain a customer's trust. They make it easy for customers to file complaints or get help resolving privacy issues, limit the sharing of personal information and implement uncomplicated privacy policies. Privacy matters to everyone. Misused personal information can have a devastating impact on individual lives (Waldman, 2018).

Emerging global regulations, such as the GDPR, further complicates the privacy and security of customer information. The regulations outline mandatory security measures for protecting customer data containing personal information for certain individuals anywhere in the world. As such, organizations in Somalia need to be conversant with the security and privacy controls described in the regulations to be compliant. In any case, the controls enhance data security. Maintaining privacy and strong protection for customer data can be achieved in different ways, which is why this research will investigate whether private and public entities in Somalia have deployed robust measures for protecting customer data.

Steps that can be taken to ensure a customer's information security (Richmond, 2012):

Conduct a data privacy audit: determine if only the required data is collected in order to prevent storage of excess data and understand the methods by which this data is stored. A data audit also identifies insufficient measures for preserving data privacy, as well as identify missing controls required to prevent unauthorized access, use, modification, deletion, or sharing.

Minimise data collection and improve protection: organisations tend to collect large amounts of information, even information it may not need, and this tends to increase risks. For example, it is unnecessary to collect dates of birth for the purposes of selling a product. In this sense, organizations require to develop and enforce data collection, storage, sharing, and discarding policies to ensure they only collect and store data vital to rendering a service or product.

Secure data: provide a secure network, databases and websites to maintain customers' trust. Companies should implement proactive measures rather than reactive procedures to identify threats and eliminate them before they can impact sensitive customer information. Moreover, they should establish a cybersecurity culture where everyone is aware of the best data protection practices to gain customer trust. Cybersecurity awareness campaigns should place data protection strategies at the center of a training program.

Communicate with customers: post a simple and clear description of a company's privacy practices for customers. Communicating to customers directly is an effective way of demonstrating transparency and dedication to leaving no stone unturned in protecting sensitive customer information. As a result, customers will have confidence in the cybersecurity measures deployed to protect their data, as well as ensure employees collecting the data remain aware of new methods for preserving data privacy.

Provide a forum for complaints: create a medium where customers can communicate their privacy issues and concerns directly and guarantee a timely response and resolve. It reassures customers that their information privacy will be preserved since their complaints, if any, will be addressed. Customers should not experience bouts of insecurity over the security or privacy of their data.

Product Information

Due to an increasing reliance on connected products, all industries are vulnerable to cyber risks. With executive engagement, control systems could be in place for the intellectual property of an organisation (Wright, 2019). In Somalia, for instance, online mobile payment products created in the diaspora but used to serve the locals are proliferating. Applications and devices require to collect and process vast amounts of sensitive personal data to operate. Other connected products play an essential role in running critical operations in private organizations or the government.

Information, such as patents and intellectual property, is valuable to attackers since it describes right of ownership of certain products. It is essential for vendors to

enhance the security of product information since it is a major motivation for attacks.

Application and cloud security is an important concept for protecting product information. Organizations in Somalia require to implement diverse cloud and applications security measures to ensure adequate protection of product information. The following are some of the applications and cloud security measures organizations should observe with respect to protecting product information:

Web applications and services security: It is a process of securing online services and websites from various cybersecurity threats that exploit vulnerabilities present in a web application. In particular, it is implementing security measures surrounding web services, such as APIs, and web applications.

Security of sensitive data exchange servers: Ecommerce has taken root as a preferred method for selling and purchasing different products and services. Multiple organizations in Somalia have developed websites to increase their business prospects and reach a larger market. As such, organizational servers hold and process vast amounts of sensitive customer information. It is crucial that the sensitive information exchanged through the servers is secured. Server security is the protection of resources and data stored in servers and comprises techniques and tools for preventing malicious activities, such as hacking and intrusions.

Collaborative tools security: These are tools used to increase productivity by enhancing collaboration among employees and team members. Examples include document sharing services, Voice over Internet Protocol (VoIP), and video conferencing tools. In spite of their obvious benefits, they provide attackers with multiple entry points and create possible vulnerabilities. Therefore, organizations need to understand collaborative security concepts, which is a recommended method for resolving security issues inherent in distributed environments. Collaborative tools security strategies include vulnerability detection, botnet resistance, spam filtering, and internet protection.

Centralised agile management solutions to configure security policies: Agile development is a methodology used to develop a product over a series of iterations.

Developers integrate and reintegrate feedback continuously during a product development lifecycle resulting in rapid development and deployment.

However, implementing security can be a headache since it requires security integration at every development phase. Hence, organizations following the agile methodology require a centralised agile management solution to ascertain security has been incorporated in all development stages.

Secure access to business resources: Digital products should provide secure access to business resources. The resources include network connectivity, customer or supplier data, cloud services, and email systems. As such, they should contain hardened security least attackers exploit existing vulnerabilities to access and steal sensitive information.

Communication levels classification and approval system: Similar to data classification, organizations should classify communication levels to determine which ones require higher security. For example, products used for communication among C-Level executives should contain advanced encryption protocols to prevent eavesdropping and man-in-the-middle attacks.

Security policies on a strategic level: Organizations should develop and maintain cybersecurity policies on strategic levels. For example, there should be an organizational or master policy, which is a blueprint for the cybersecurity practices and procedures across the entire company. Also, a system-specific policy for specific products should be developed to provide the required controls and countermeasures for enhancing the security of software or hardware.

Encrypted IP traffic visibility: Encrypting IP traffic visibility is essential to protecting an organization’s internet activities from prying eyes. Organizations should consider encrypting their IP traffics by implementing SSL and TSL security on all web-based products.

Traffic monitoring and evaluation: Monitoring web traffic is a recommended practice for identifying malicious user activities. Some malicious insiders pose a huge threat to system and information security since they have permissions to access certain

assets. Implementing monitoring solutions and tools for evaluating and analysing user activities can enable an organization to keep ahead of malicious users.

Employee Information

To maintain employee relations, organisations collect sensitive information about their employees. From medical records and date of birth to the personal identification number of employees, employers keep it all. But it is a big responsibility to protect this type of information (Halpern, 2010). In today's digital world, data is the new currency. Companies that fall victim to cyberattacks lose more than money: they lose the confidential data of their customers as well as their employees. Other consequences like a damaged reputation have far-reaching impacts since employees and customers alike mistrust a company's ability to secure sensitive information.

Somalia is registering a swift growth of digital technologies due to a relatively peaceful environment in the past few years. More organizations are springing up providing employment to many people. The downside is Somalia is among the countries with poor cybersecurity practices due to a lack of proper cybersecurity legislations and standards stipulating the required measures and controls for protecting sensitive employee information.

The public sector is the most affected since at least 80% of attacks in Somalia target government employees and agencies. A similar problem exists in the private sector. Therefore, understanding theories regarding the required practices when protecting employee information is vital to the success of the research. Some of the following theories will be applied in evaluating the measures and controls used to secure employee information in Somalia and recommend countermeasures for addressing existing cybersecurity and awareness challenges (Anderson, 2001):

Develop IT security policies: developing formal security policies that identify the type of employee information the company will protect and update it on a regular basis. Make it clear to employees that their data will not be used for any other purpose other than business. Somali organizations should consider the most appropriate IT policies that meets their business and security needs. An employee privacy policy, for

instance, may contain employee privacy protection requirements, such as the details or types of privacy information the employer may collect, a detailed description of what comprises of employee personal data, detailed employee information collection, use, and processing procedures, and a description of how the employer can handle employee disputes regarding the information's privacy.

Educate employees: employees could be the reason for data violation. They need to be educated in terms of their value and ethical responsibilities towards the organisation they work for. Furthermore, make it clear that unapproved duplicating, sending, surveying or utilisation of delicate worker data will lead to severe consequences, such as termination of employment and legal action. In addition, employee awareness in handling and protecting other employee information privacy is pertinent to preserving its confidentiality, availability, and integrity. Employee errors and lack of awareness in protecting data is the single-largest cause of data breaches and theft.

In this case, each department within an organisation should develop and maintain robust and unique procedures for ensuring employee information remains protected. For instance, the finance department should maintain policies guiding access and use of other employee data when preparing payrolls and other payment schemes.

Restrict access: applying limitations to the availability of data is another way to keep it safe. The accessibility of information should be characterised firmly according to the roles of the employees. E.g., managers should only be able to access performance parameters and information. During the research process, an essential factor to consider is the measures applied to prevent unauthorized access to confidential employee or customer information.

The measures should consist of information access controls, such as role-based access control, where a user should only access data facilitating the completion of a specific task. Other organisations use mandatory access controls, where a central authority, such as a system admin, is responsible for granting or restricting access to employee information to different users. There are many other controls and

measures for restricting access to employee data, and this research will establish the current implementation levels in Somali entities.

Investigate incidents promptly: if someone may have accessed sensitive information, then initiate a proper and rapid investigation. At this point, all the security policies need to be revised and it should be determined if any betterment is required to safeguard employee records. All investigations must be done within the shortest time to identify and resolve vulnerabilities or insufficient policies causing the challenges. Depending on the magnitude of the incidence, a company may use its inhouse security team to conduct the investigation or outsource the services to a larger cybersecurity team containing the required expertise and resources for performing an in-depth examination of the affected information systems and make appropriate recommendations for maintaining sufficient employee information privacy and security.

Dispose of records properly: employers must impose the practice of disposal of all employee records at the end of the retention period, so that they can no longer be accessed. Moreover, ensure the elimination of electronic media containing the employee information. As such, all organisations need to establish data disposal privacy for employee information stored in digital or paper format. Among other things, an information disposal policy should include the preferred data destruction methods to ensure information no longer required is deleted and discarded completely.

Furthermore, a data disposal policy is essential since it states the amount of time an organisation should store employee data after an employee has left the company. Such a requirement ensures that employee information does not fall in the wrong hands or used for purposes other than those stated when collecting it. An organisation must ensure employees are aware of such policies to assure their data will remain secure.

Company/Organisation/Government Information

Confidential business information is sometimes referred to as ‘proprietary information’ or ‘trade secrets’. This is information that is sensitive and should not be

accessible to competitors or to the public. It might include manufacturing processes, business plans, budgets and forecasts, financial data, ingredient formulas and recipes, supplier or vendor lists, and employees or customers lists (Anderson, 2001).

Protecting company or government information should be a priority of all entities in Somalia. A significant number of attackers and data breaches target valuable information due to the obvious monetary gains. For example, an enemy state can sponsor hackers with the required resources to conduct cyber espionage to gain trade secrets, economic, or military information in order to gain an upper hand.

On the same note, a rival company can sponsor attackers to hack another organisation to steal patents or intellectual property, which can enable it to steal ideas on creating innovative products or claim ownership of products already in the market, respectively. As such, understanding the best practices and required procedures for protecting company or government data is critical to meeting the research's objective of evaluating cybersecurity state and awareness in Somalia.

Recommended security points are as follows (Chubb, 2019).

Accessibility of records: confidential information should only be accessible to the relevant employees. Data restrictions or limitations should be implemented. In this case, the research will evaluate and assess some of the access control policies mentioned in protecting employee information. They include discretionary access control, role-based access control, attribute-based access control, rule-based access control and mandatory access control. All private organisations and government agencies should implement and maintain at least one of the required policies and controls to safeguard high-value data from unauthorised access.

Data protection policies: investing and implementing security firewalls and encryptions should be carried out. All security policies and plans should be reviewed to ensure compliance with state law. In contrast to the access policies that govern the users permitted to access which type of information, data protection policies outline and describe the minimum controls required to maintain a certain level of data security. There are many types of data protection policies Somali organisations must enforce and adhere to in order to maintain sufficient data protection. Some of

the policies to be assess in the research include encryption policies for data at rest, in transit, and in use. An acceptable use policy is pertinent to preventing users from misusing essential government or company data. An acceptable use policy restricts employees from using confidential data in insecure environments or sharing them with unauthorised individuals. Other types of data protection policies include password policies, email polices, and data processing policies.

Bring-in a Non-Disclosure Agreement (NDA): Another way to implement or enforce security policies is to create an agreement that has to be signed by all employees within the organisation. The agreements provide protection to confidential and private information and they restrain employees from sharing such sensitive information. In the case of a data breach, legal action can be taken on the basis of these agreements. Therefore, Somali government agencies and companies in the private sector should ensure all employees or users, including contractors and suppliers, with access to sensitive information sign an NDA.

An NDA serves as a vital legal framework through which Somali entities can protect confidential and sensitive information from being shared with or made available to any other person or entity. NDAs are especially essential to start-up companies since they ascertain the protection of new innovations and ideas.

3.5 Cybercrimes

3.5.1 Definition of Cybercrime

Criminal activities that take place in cyberspace and are intended to harm individuals or organisations through network devices are referred to as cybercrimes. Most of them are committed by hackers or cyber criminals, purposely to make money. The reason for such an act could also be personal or political. Cyber criminals are highly skilled and use advanced techniques.

Somalia is among the countries with a low cybersecurity index both globally and in the region, implying it bears the brunt of cyber-attacks. Different types of cybercrimes exist and driven by various motivations. Monetary gain is the primary motivational factor followed by data breaches targeting highly-sensitive information.

In this regard, the research will establish the most pervasive cybercrimes in Somalia that affect the government, private, and other sectors in the past years. Therefore, it is essential to dig deeper into some of the most common cybercrimes today to better understand them. Some common examples of cybercrime are (Anderson, 2001):

Digital fraud: Digital fraud encompasses all fraudulent schemes executed with the aid of digital technologies and internet services with the intention of defrauding targeted individuals. Attackers execute the scams use various techniques, including social engineering methods.

Identity theft: Identity theft is a type of cybercrime in which a malicious individual obtains and uses the personal information of another person without their consent. There are many types of identity theft cybercrimes, such as stealing credit card information of a victim and using it for malicious reasons. Also, using the medical information of a patient to defraud a health insurance provider is another example of identity theft.

Cyber espionage: Cyber espionage, popularly known as cyber spying, is a type of a cybercrime used to obtain sensitive and secret information from competitors, individuals, governments, groups, military, or rivals. Cyber espionage facilitates other crimes, such as stealing trade secrets or patents.

Crypto jacking: Attackers execute crypto mining attacks by creating, disseminating, and distributing malware programs designed to use a victim's computer or network resources to mine for cryptocurrencies. While the attacks are not harmful in nature, they can disrupt critical operations since heavy usage of resources can mean unavailability for other functions. The attacks cause slow system performance, extremely high CPU usage, and network unavailability.

Credit card credentials theft: As the term implies, this is a type of cybercrime used to steal credit card credentials for use in unauthorized purchases. The methods used to execute credit card theft include the use of skimming devices, social engineering tactics, spyware and malware infestations, and shoulder surfing.

Selling of corporate data: Once a cyber espionage attack is successful, attackers can choose to sell the stolen data for financial rewards. The data can be sold to business competitors, enemy nation states, or on the dark web to the highest bidder.

Cyber extortion: Cyber extortion is the use of blackmail or threats to get something out of someone. For example, a rival business can use embarrassing pictures to force a competitor out of the market. Cyber extortion crimes are pervasive since hackers use anonymous sites and tools to hide their identities, making it difficult for investigators to track the perpetrators and bring them to book.

Ransomware attacks: Ransomware is a common example of cyber extortion schemes. Ransomware attacks involve the use of malicious programs to encrypt company or government data until the affected entity pays a ransom, mostly in the form of bitcoins. The attackers use threats, such as sharing the encrypted information in the dark web or deleting it, until the ransom demands are met.

3.5.2 Data/Information Crimes

Data Interception: this is a type of data or information crime in which the attacker keeps an eye on the data and target to gather information to use it later, or sometimes only this collection of data might be the end goal. In this form of data crime, the attacker is not the intentional recipient. This is not like other attacks in which more qualitative information is gathered (Lebied, 2018). Data interception can also be described as techniques for obstructing information being shared from reaching the intended recipient.

Hackers use various techniques to intercept data, with the most common one being the use of a hijacking software and pretending to be destination within a network. Other methods include sniffing a network using a specialized hardware or software to monitor a target's network traffic and intercepting data packets deemed important. For a data interception attack to be successful, hackers exploit network vulnerabilities to listen on communications between different parties.

Data Modification: in a data modification attack, an unauthorised party on the network interrupts data and changes parts of that data before re-transmitting it

(Ahmed, 2015). Data modification often relies on the success of a data interception attack to enable malicious adversaries to modify the intended data before sending it to the intended destination. Data modification attacks result in adverse implications for the affected parties since they may end up revealing sensitive information to the attacker while thinking they are sharing with each other. Other motives for a data interception attack include altering the comprehension of an intended message for various malicious purposes and preventing the recipients from receiving crucial information.

Data Theft: the illegal capturing or copying of data of individuals or businesses is referred to as data theft. When the cybercriminal or attacker is detained, he must be punished according to the law (Lord, 2018). Attackers use a variety of methods to steal valuable data. Any attack that results in lost information or data exfiltration can be termed as a data theft attack. The attacks range from simple methods, such as social engineering attacks, to more comprehensive malware attacks. Organizational employees stealing company data for whichever reason perpetrate insider data theft attacks. As such, Somali organizations should implement and deploy adequate measures, policies, and controls to ensure the security of all data types.

3.5.3 Network Crimes and Access Attacks

Network Interferences; modification, disruption and deletion of data by compromising the networking protocols (Rout, 2008). Also, network disruption attack is a deliberately malicious act to harm equipment or create disruption in the normal functions or processes of the network (Swami, 2017). On the other hand, unauthorised access attacks are used to gain access to someone else's account, server, or system without the owners' explicit permissions (Computerhope, 2020). Attackers also use virus dissemination attacks to execute access attacks. Virus dissemination involves sending or attacking with malicious software or viruses to gain unauthorized access to a protected system or data. It usually destroys the system of the victim (Venkat, 2016).

3.6 Impacts of Cybercrime

Today, organised crime groups are using cyberspace for major scam and theft activities. Internet-based crime is becoming more common, as criminals shift away from traditional methods. This increase in cybercrimes is due to the high usage of the Internet for shopping, business, etc. In 2004, cyber criminals made much more money than drug suppliers, and this is expected to rise as the use of technology is increasing in developing countries (Ross et al., 2012).

Scott Borg, the director of the U.S. Cyber Consequences Unit, recently proposed that viruses are considered 'not quite mature' when compared to the potential of attacks in future (Saini, 2012).

3.6.1 Potential Economic Impact

A report in 2011 by the Norton cybercrime unit revealed sad news. According to Norton, more than 74 million citizens of the United States were found to be victims of cybercrime in the past year, which directly resulted in a $32 billion financial loss. Later, it was further revealed that 69% of adults are the victims of this crime, which can be calculated as one million crimes per day. Many people think cybercrime is due to online business. According to the survey, 80 percent of the companies have incurred a financial loss because of cybercrime (Norton, 2011).

Approximately, this has resulted in $450 million of computer breaches. We learn about new attacks every week on computer system safety, integrity and availability. This may involve hacking and leakage of personal information. As the economy builds on the Internet, cyber criminals are exposed to all attacks. Stocks are exchanged via the Internet, trading is done on the Web, buying via credit card is done via the Web. All fraud cases in these transactions have an effect on the company's financial condition and thus on the economy (Monica et al., 2014).

One of the major impacts and a significant concern is the instability of international financial markets. Various countries and time zones dominate the global economy. Such interdependence of the global economic system would have a ripple impact in other regions, not just one area of the world. Any interaction with these systems will

then transmit shock waves outside the market that caused the problem. Attacks on these global markets can halt trading, disrupting operations and causing major financial losses.

The user will sacrifice valuable time due to attacks by worms, viruses, etc. Machines could operate more slowly, servers could be unavailable, networks could be disrupted, etc., even when the external client finds the company to be a detrimental factor. Moreover, consumer anxiety about possible fraud prohibits purchase for a large cross-section of online shoppers. There is no question that a large share of e-commerce revenue has been lost by buyers' concerns and worries (Ashford, 2018). Also at risk is the public confidence in these markets. There will be a reduction in public trust in these online shopping avenues leading to less participation, and thus total less revenue generated.

Business Continuity

Cybercrime involves a variety of illegal criminal activities to abuse the information protection of the organisation. The electronic break may be intended to deprive the company or its customers of their financial information, or to deprive the service of the company website or to install a virus that tracks the operations of a business online (Arnold, 2017).

We must invest a fortune so that businesses are able to defend themselves against cyber criminals. Risks are detected, safer and most optimal operating procedures are developed, and safe and secure hardware and software are availed, which also means employing a proper cybersecurity contractor to create a personalised approach for companies with advanced and complicated or sensitive operations. The initial security cost is not the only outgoing as systems must be constantly checked and monitored to ensure that they continue to be successful in the face of emerging cyberattacks (Becker, 1968).

The cyber activist has formed a new culture in the last few years. These are the online equivalents of demonstrators who scale up buildings or trees. They aim to black out the online busines and marketing of a company and send a message about online business. In the past two years, significant businesses have been targeted in

the same way, such as MasterCard and PayPal. Dozens of people claiming to belong to the party, Anonymous, targeted the PayPal website in December 2010.

In response to PayPal shutting down payment services to Wiki Leaks, they tried to carry out a denial of the service attack. Over a dozen hackers were arrested (IS forum, 2011). While PayPal has not been shut down, several other companies are not so fortunate. An attack on an online store leads to less sales for a company as customers cannot access their goods and services. It may also contribute to lower long-term profits if some clients decide to quit doing business with a vulnerable company.

3.6.2 Impact on Market Value

The economic effect of security violations is in the interests of both companies that try to determine where and insurance firms providing cybersecurity policies. This changing view of harm is more important, as many organisations rely on the Internet to manage their enterprises. This precedent will gain the liability for hacker attacks and other security violations for several insurance firms. Some industry executives agree that the prices for such plans are largely dependent on creativity. Industry experts note the need for improved ROSI studies that can be used to build hacking insurance companies (Monica et al., 2014).

A new approach to assessing the likelihood of infringements of safety is therefore required. However, one approach is to calculate the effect of a violation on a company's market value. A value approach illustrates the expectations of the stock market for damages arising from the infringement of protection. The reason for this is that businesses are always influenced more by exposure to public attention than by the attack itself. In addition, managers attempt to increase the market value of a business by investing in projects that either improve their value or reduce the risk (Becker, 1968).

3.6.3 Impact on Consumers

Consumer Trust

Since cyber criminals infiltrate other areas and attempt to attack the different web pages, the customer visiting the website concerned is irritated and discouraged to make long-term use of the site. The site in question is identified as fraudulent, but the root cause is not recognised as the criminal responsible for the secret attack, which results in the loss of customer trust for their website and for the Internet (David, 2008). Almost 80% of online customers have mentioned protection as a primary concern when doing business on the Internet, according to research published by the Better Business Bureau Online (Angraini, 2019).

When asked for credit card details, almost 75% of customers complete their online purchase (Steele, 2019). This has become a very big issue for the e-commerce industry. The issue was compounded by customer perceptions of fraud that the situation was critical. Market knowledge may be a positive or negative reality. This prohibits users from investing in a company concerning fraud. A shopper is hesitant to deal with questions regarding the reputation of an e-company regarding its dangerous and embarrassed nature (Monica et al., 2014).

Consumer Data

Cybercriminal users are highly worried about people and cultures. Present cost estimates are still inaccurate and there is no agreement on effective methods of calculating this. The measurement of social costs helps to prepare initiatives against crime. Traditional offenses need accurate assessments for advising legislation, prioritising compliance, and tailoring public education.

Furthermore, the performance of commonly implemented security measures can be evaluated. Customers usually lose not only their money due to these cyberattacks but also their personal data, which poses a risk of potential violence (Smith, 2004).

3.7 Conclusion

This chapter analysed the threats affecting internet usage and cyber space. This was based on the three principles of information security: confidentiality, integrity and availability. We analysed different types of cybercrimes such as digital fraud, identity theft, cyber espionage, crypto jacking, credit card credentials theft, selling of corporate data, cyber extortion and ransomware attacks. There was also an analysis done on data/information crimes such as data interception, data modification and data theft.

This analysis helped us understand how big the attack surface is and how many attack vectors are there. Attackers are usually after data and have multiple ways of obtaining it. The CIA triad mentioned earlier provides the perfect foundation to protect this data.

We examined four types of information, that is, customer information, product information, employee information and company information with an emphasis on the steps that can be taken to ensure their security. Analysis of this information will help guide the creation of the survey as we shall be asking the individuals and institutions if they have taken a couple of these steps to ensure their information is safe.

With emerging global regulations like GDPR and the increased use of cloud services and applications, protection of information is of utmost importance. Key steps in securing this information include securing data with proper controls such as by use of encryption. These controls should be set for all types of data. There ought to be a set of IT security policies dictating the use and access of this data and all users of such data should be educated on how to properly access, handle and dispose of the data.

We considered different types of cybercrimes as well as their major impacts. We focused on economic impacts, impacts on market value and the impact on consumers. They range from a general disruption of the global markets to disruption of individual businesses. It stands to reason that most cybercrimes often lead to a loss of finances in one way or another. Understanding the impact of cybercrimes provides further justification for this thesis. The impacts of cybercrime are very

massive, and knowledge of this information validates the need for cyber awareness analysis and improvement.

4 Cybersecurity in developed and developing countries

The main criteria that dominates the split between a developed country and a non-developed country is economic development. The classification of countries is based on the economic status of the country as well as the standard of living within that country. A developed country typically implies a developed economy, with a high level of wealth and resources available to its residents or citizens while developing countries have low and middle-income economies.

Cybersecurity challenges have gained popularity worldwide. The developed countries have made massive progress by improving cybersecurity regulations, forming cybercrime response teams and cyber security education for end-users. Other nations are becoming more informed at international level about how cybersecurity may impact their sensitive and critical data and their connections with other nations (ITU, 2005).

The case studies from the developed countries are: United Kingdom, Canada, United States of America and Australia. These were chosen from 3 different continents in order to explore a wide range of different ideas. They were also selected as they are all in the top 10 countries according to their Global Cybersecurity Index (Statista, 2018). Looking at the developed countries can offer learning opportunities to Somalia so that it can map out a path to cybersecurity excellence.

The case studies from the developing countries include Mauritius, Rwanda and Egypt. They were selected because they have successful on-going cybersecurity initiatives. Looking at developing countries can provide starting points as they have employed innovative strategies and well-aligned policy instruments, despite the presence of less capital.

The cybersecurity priority of developing countries is to protect their citizens and business from online threats as opposed to the focus on CIIP (Critical Information Infrastructure Protection) by the developed countries. These is because the

developing countries are yet to build these infrastructures. This information collected within this section will help guide the recommendations provided within the thesis in order to provide commendable tested solutions to issues identified. It will help guide Somalia in creating a national cyberspace defense strategy and plan, by drawing lessons from the working initiatives in other countries. Looking at a wide variability of countries provides options, as there is no one solution that fits all nations. The research thus reveals common elements of effective cybersecurity strategies. These include:

- Increased funding/ budget for cybersecurity.
- A dedicated national cybersecurity agency.
- Creation of a cybersecurity awareness culture.

4.1 Cyber Security Initiatives in developed countries

The developed countries have a high interest in cybersecurity and tend to invest very highly in this area. They have advanced cybersecurity awareness programs to reach out to the general public and improve the general cybersecurity culture. They set up national cybersecurity agencies to collect and share information on cybercrimes and curtail their spread. They also have comprehensive ICT and Cybersecurity policies and plans. These governments actively monitor cyber threats.

In this section, cybersecurity efforts of four developed countries are listed.

4.1.1 The United Kingdom Blueprint

The United Kingdom is one of the largest digital nations in the world. Much of their success depends on their ability to protect their equipment, data and networks from the many threats they face. Still, cyberattacks are growing more common, complex and damaging. The UK strategy is world leading (ITU-GCI, 2018) because of its extensive scope and bold vision. Additionally, it stands out by being implemented through a structured programme accompanied by the transformational investment of £1.9 billion (NCSC, 2016). This investment represented a doubling of the funding compared to the 2011–2016 period (Young, 2016). It is intended to make Britain optimistic, competent and resilient.

Crucial action is still required to protect the privacy and economy of UK civilians. A review policy is in place to better respond to the threats, in addition to the evolution of security technologies. These risks cannot be entirely removed, but the risks can be minimised to a degree that allows society to continue to prosper and take advantage of these splendid offers presented by the digital market (Boston Consulting Group, 2015). Constant review of the policies is necessary as the cybersecurity landscape is ever changing.

In 2013, the Cyber Security Information Sharing Partnership was launched. This allows the government and the private sector to share information on threats swiftly and regularly. Information sharing has long been viewed as essential to cybersecurity and it can help provide early warning signs, as well as prevent the same attack from re-occurring. This situational awareness of cyber threats is very important to both the private sector and the government.

In October 2016, the UK government launched the National Cyber Security Centre (NCSC) to enable all citizens and institutions within the country to report cyber security incidents. Shortly after the formation of the NCSC, the National Cyber Security Centre strategy was created. The strategy included an Active Cyber Defence Initiative that was aimed at reducing the number of cyber threats within the UK. This automated solution provides security services such as:

- Takedown services for malicious content hosted within the UK.
- DMARC for email security and spoofing prevention.
- Website vulnerability checks
- Public Sector protective DNS services.

The NCSC also launched a Cyber Aware campaign to improve online security by protecting accounts and devices from cybercrime. This is done by focusing on password use, updating device software and backing up of information. Considering the total cost for a small business of an information security incident is estimated at £10,000–£20,000. It can be £1–2 million (Information Security Breaches Survey, 2008) for a large organisation with more than 500 workers. Alongside scammers, the online space is threatened by violent criminals and terrorists, which demands

additional vigilance in terms of a cybersecurity strategy. That is why cyber security is the most useful for the UK to fight and defeat crime and terrorism. Considering its importance, the UK government is investing heavily to educate and spread awareness of cybersecurity (Hankin, 2017).

The UK Cyber Security Strategy 2016-2021 is based around the themes of 'Deter, Defend and Develop' in this fast-moving digital world. The strategy has a main objective of developing cyber skills within the cybersecurity sector. These range from cybersecurity awareness information for the general public, to workshops and trainings for the workforce and institutions. Cyberspace is connected to all security threats in the National Security Strategy, even with international agencies. Multiple institutions, both governmental and private, are beneficiaries of a networked society made possible by a connected and cybercrime-free Internet (Hankin, 2017).

Furthermore, international partners are engaged in collaborated efforts to contain cyber threats. With the UKs departure from the European Union, there is an increased effort to maintain the partnerships once held and create new ones. Considering the importance of cybersecurity, more than ever before, the UK has invested a lot of effort in improving the cyber infrastructure. However, a lot of effort is to be executed in the coming years, especially regarding awareness of cyber security. These initiatives would bring improvements in cybersecurity and the cyber industry for the purpose of education, research and development (UK-OC, 2009).

4.1.2 Canadian Blueprint

The digital world is rising sharper than the conventional economy. In 2015, the global Internet economy is projected to be worth $4.2 trillion (Boston Consulting Group, 2015). Canada has a GDP of $1.83 trillion and has a 3.6% Internet economy, which does not consider any data value. Digital economy growth and record keeping digitisation have fueled a rise in the number of cyber criminals seeking to steal data (The Heritage Foundation, 2020). In Canada, there are a growing number of companies suffering cybercrime losses.

The famous Ponemon Institute has evaluated almost 24 IBM organisations in all sectors (IBM, 2016). Its findings are:

- Net data breach costs $6.03 million.
- The average cost is $258 per breach record.
- The mean number of records infringed in 2016 was 20,456.

Through the 2018 federal budget, the federal government provided funding to revamp Canada's national cybersecurity system and develop the Canadian Cyber Security Centre, based within the Canadian Security Department, and the National Coordinating Unit for Cybercrime. These two new agencies will collaborate with the Public Safety and Emergency Preparedness Agency, which remains in charge of national planning and strategy. In June 2018, the federal government also launched a new National Cyber Security Policy (IBM, 2016).

The Canadian Cyber Security Centre includes the Canada National Computer Security Incident Response Team that is responsible for responding to cybersecurity incidents within the country. The Canada CSIRT also provides cybersecurity awareness content through the Get Cyber Safe campaign. The goal of this campaign is to increase Canadians cyber hygiene by providing simple steps to protecting oneself and devices.

One area of Canada's national cybersecurity strategy for 2018 is ‘cyber creativity’, which includes ‘funding for innovative research and development of cyber skills and information’. The committee recommends that this theme become the strategy 's focus and provides a roadmap to improving cybersecurity education and the value of cyber resilience within Canada.

Canada has several laws and regulations that help foster cybersecurity resilience within the country and protect its citizens. These include: The Privacy Act, The Access to Information Act, The Personal Information Protection and Electronic Documents Act, and Canada Anti-Spam Law. Along with this, it is important to balance the need to encourage and foster emerging technology and opportunities such as skills growth, research and development funding, and education for the general public and companies (Senate Canada, 2018).

4.1.3 The United States (US) Blueprint

A cyberattack can be a potential reason for raising many issues, e.g., cyber theft, online crimes, and communication outages, etc. However, major improvements are yet to be implemented in securing US cyber networks from the government authorities. US congress is unable to come to an agreement when it comes to striking a balance between network security and privacy. Moreover, there is a lack of communication among various organisations due to a shortage of funding. Government and private organisations are yet to have a communication process along with requisite funding to effectively address the cyber threats in the US (Homeland Security, 2020). At $9.85 billion, the USA has one of the largest cybersecurity budget in 2021. This illustrates the high prioritization of cybersecurity within the country.

A new Cyber Information Sharing and Security Act (CISPA) law was adopted in 2011. CISPA's concept of a cyber-threat is very clear: 'an effort to undermine, damage or kill the device or network' or 'theft or misuse of private or personal information or intellectual property or government information' (U.S. H.R. 624, 2011). In order to address valid concerns of various civil liberties categories and other privacy advocates, the bill was amended with the provision of lawsuits against the US Government in cases of privacy violations (Flaherty, 2013); (U.S. H.R. 3523, 2012).

The bill is still pending approval from the senate with the US government and private organisations pushing towards early approval. Moreover, the Electronic Crimes Task Force (ECTF), a special Secret Service unit, is there to combat cyber-attacks/criminals. Cyber intrusion, data breaches, bank fraud and other kinds of cybercrimes, along with the credit card theft numbers, are all addressed by this task force (Combat Cyber Crime, 2014).

The US National Security Operations Center within the National Security Agency (NSA) is always on high alert, monitoring all security threats both within and towards the United States. The FBI’s National Threat Operations Center acts as an intermediate for receiving security incidents within the United States.

It has been observed that the challenge remains in communication with hacking threats for private and public organisations. A mechanism is to be established to alarm organisations across the US in relation to cyber threats from any susceptible software. In North Carolina, an owner of a small tech firm tested the cybersecurity of computer networks owned by a power company. Penetrating their servers was surprisingly easy. It was also noticed that the shutdown of power grids was possible without much effort from this hacking (*The News Tribune*, 2014).

The Department of Homeland Security created the Cybersecurity and Infrastructure Security Agency (CISA) to protect the nations critical infrastructure by addressing any cybersecurity issues. This organization provides information on current threats within the cyberspace, providing tips and alerts to the general public and businesses. CISA was also created to identify threats and assist with incident response. With a main mission of building the national capacity to defend against cyber-attacks, CISA places very high emphasis on cybersecurity awareness.

There are also a large number of organisations that provide cybersecurity awareness within the USA such as the NICCS (National Initiative for Cybersecurity Careers and Studies), the NCSA (National Cyber Security Alliance) and the NCS (National Cybersecurity Society) Despite being a developed nation, the United States of America needs to do a lot of work on cybersecurity, there are unaddressed issues in legislation, communication and proper funding.

4.1.4 Australian Blueprint

In Australia, the economy is rapidly evolving, generating new industries and dramatically reforming existing ones. Australia has a competitive advantage in the vital cybersecurity environment as conventional borders disintegrate. A strong and competitive Australian cyber security sector will not only reinforce the future growth of all Australian industry, but a new economic pillar will also be introduced (Austrailian Government, 2020).

As Australia aspires to become a global leader in this area, they are developing this industry with skills from their world-class education system, test beds backed by their limited but sophisticated market and an alliance of cultures and time zones in

their geographic region. Via the Indo-Pacific, Australia uses its work in common languages and business hours as an added benefit. As Australia reacts to major global disruption, a strong domestic cybersecurity field will not only allow Australia's economy to expand but will also build an opportunity to outstrip the world stage (CSIRO, 2018).

Engagement in cybersecurity by the government would help companies diversify and build new markets, setting the groundwork for a productive future. The government will also help Australia's cybersecurity industry to extend and promote their skills to the global market and take advantage of the rising global demand for cybersecurity services. At home, good cybersecurity services will promote trust and confidence in digitally operating Australian businesses. With better oriented research and development on cybersecurity that responds to industry and government needs, Australia will generate investment, employment and improve their national cybersecurity. It would also make Australia a more economically appealing destination (Australia's Cyber Security Strategy, 2016).

Australia's government seems committed to allowing for creativity, development and prosperity through good cybersecurity for all Australians. This is in line with the wider National Innovation and Science Agenda of the Australian Government to help make Australia a new, diverse 21st century economy.

This plan sets out five principles of action for cybersecurity in Australia by 2020 (Australia's Cyber Security Strategy, 2016):

- A global alliance on the cyber.
- Solid cyber defenses.
- Global obligation and impact.
- Growth and novelty.
- A smart nation on the Web.

4.2 Cybersecurity in Developing Countries: Africa

Today, everything is connected to the Internet, and every part of our lives is dependent on the Internet. Some of the developing countries in Africa started

preparing to develop their national cybersecurity frameworks after increased the use of telecommunication and mobile devices (Aker et al., 2010). Examining efforts in developing countries is very crucial to this research as Somalia is a developing nation. Understanding what countries with an equal state of development as Somalia are doing provides easier and faster approaches to dealing with cybersecurity in the country.

Most of the developing countries have little to no capabilities and infrastructure in terms of cybersecurity, but many of them in the process of creating the cybersecurity policies or in advanced stages of implementing them. South Africa became the first country to release a draft cybersecurity policy, followed by other countries in the continent (Ewan , 2017). The three analysed countries also have Computer Emergency Response Teams that inform and assist the general public and organisations in implementing measures to decrease the risks of cyber threats. In this section, cybersecurity efforts in some developing countries are listed.

4.2.1 Mauritius

Mauritius has been working with a cybersecurity strategy since 2014. In its cybercrime strategy 2017, the government recognised the severe threats coming from cybercriminals. Their national cybersecurity strategy was approved in 2014 by the Cabinet. Mauritius is one of the countries in Africa that is actively involved in the capacity building of its cybersecurity program, the reason being that they have developed a setup of the ICT and telecom sectors (First edn, 2014).

Mauritius's cybersecurity strategy states that cybersecurity management should have a reliable and real-time awareness about security alerts impacting key functions of society. The first fundamental principle of the strategy is to make cybersecurity a comprehensive part of society, while its cybersecurity effectiveness relies on the security preparedness of the entire nation (First edn, 2014).

The goal is to protect all the critical national information assets from all types of cyber-attacks, including both inside and outside threats. Another important part of their strategy is the establishment of the National CERT (Computer Emergency Response Team), which is responsible for implementing the outputs generated from

the cybersecurity community, to handle cybersecurity incidents, to prevent the occurrence of cyber incidents, and to promote the adoption of best practices in information security and compliance (First edn, 2014).

In 2008, the NCB (National Computer Board) created a division called the CERT-MU (Mauritius Computer Emergency Response Team) to enhance cybersecurity awareness of the general public. Mauritius's national cybersecurity strategy 2014 also suggests the guidelines for its cybersecurity implementation. According to the cybersecurity strategy 2014, some of the strategic approaches are as follows:

- To secure the cyberspace of Mauritius and establish a front line of defense against cybercrime.
- To be able to protect against all kinds of cyber-attacks.
- To develop an efficient collaborative model between authorities and the business community.
- To improve cyber expertise and provide awareness to all sectors of society.
- Encouraging youth to join the cybersecurity domain and improve the cyber expertise of the nation. (First edn, 2014)

The Ministry of Technology, Communication and Innovation is the key contact point for cybersecurity within the country. They were responsible for setting up a Cybercrime Strategy with a major objective of increasing capacity to better address cybercrime. The Mauritian Cybercrime Online Reporting System (MAUCORS) is a national online platform for reporting cybercrimes. The channel used to collect this information is social media. MAUCORS also provides awareness information on major cybercrimes and how to avoid them. The Mauritius Police force has a specialized cybercrime unit for investigating cybercrime.

There is also a Government Security Incident Response Team (G-SIRT) for handling cybersecurity incidents within the government sector. The G-SIRT created an Automated ICT Security Incident Handling System (AISIHS) for better tracking and quick response towards cybersecurity incidents. There are also several cybersecurity

laws in place, such as, the Computer Misuse and Cybercrime Act, the Data Protection Act No. 20, the Information and Communication Technologies Act 2001 and The Electronic Transaction Act 2000.

According to the International Telecommunication Union (ITU) Cybersecurity Global Index 2017, Mauritius is ranked first in Africa and sixth in the world (ITU-GCI, 2018). The government's vision 2030 is to transform Mauritius into a SMART island. This shows how well the government is performing in the cybersecurity sector.

4.2.2 Rwanda

Rwanda provided a draft report for the formation of its national cybersecurity strategy in 2015. The purpose of this draft was to define the National Cybersecurity Agency, new cybersecurity initiatives and priorities, and the duties for every party in terms of cybersecurity, as well as the establishment of a national cybersecurity strategy.

In addition, Rwanda proposed the NCSP (National Cybersecurity Policy) for the purpose of defining strong and effective cybersecurity governance in the country. The responsibilities of the National Cyber Security Agency are as follows (Republic of Rwanda, 2015):

- Implementing cybersecurity policies, strategies, and standards.
- Implementation and coordination of cybersecurity initiatives.
- Manages the Rwanda CSIRT (Cyber Security Incident Response Team), which will act as a national point of contact to coordinate the incident handling process.
- Protect the country's critical infrastructures.
- Build and improve the cybersecurity industry.
- Cooperate with international key players.
- Promotion of cybersecurity awareness.

The NCSP also defines the establishment of National Cyber Security Advisory Board (NCSA), National Cyber Security Agency (NCSA), public and private institutional ICT units with cyber security functions as well as specialized cyber security centers like the National Cyber Crime Investigation Center.

Under the guidance of the Rwanda Information Society Agency (RISA), there are 4 cybersecurity laws, namely, the ICT Law, the PKI Regulations, the E-Transaction law and the Cyber-Crimes Law.

4.2.3 Egypt

Egypt is ranked Ninth in the Global Cybersecurity Index (GCI), which shows it is slightly above the other developing countries in the world (GCI, 2018). Egypt's government released its national cybersecurity strategy 2017 - 2021 and identified the most significant cyber threats and challenges as follows (Egypt National Cybersecurity Strategy, 2017):

Threat of Infections: The new emerging threats such as malware include viruses, trojans and spyware aim to disrupt critical ICT infrastructure and are considered as serious threats by Egypt. They may cause damage to industries such as oil & gas, electricity, the communications industry and various forms of transportation, etc.

Threat of Cyber Attacks: The threats of cybercrime and cyber terrorism are emerging due to a variety of new technologies. Cloud computing provides attackers with unlimited resources and opens up more users to compromise. This increased attack surface area, coupled with increased knowledge by attackers, provides a ground for attacks. Cybercriminals can compromise thousands of insecure devices and make them part of their botnet to perform several illegal activities such as DDoS attacks, phishing attacks, etc. Egypt's national cybersecurity strategy aims to safeguard the infrastructure from cyber-attacks and cybercrime activities.

Threat of Digital Identity and Privacy Data Theft: Hackers can steal personal data using various techniques and impersonate individuals for illegal activities. Personal information can be stolen mainly from ATM card scamming, stock exchanges, e-

payment networks, etc. The threat of digital identity is one of the most severe threats, and the national cybersecurity strategy addresses this in their strategy to protect the citizens.

The 2017 cybersecurity strategy is aimed to protect the most targeted critical sectors of the country, especially the:

- ICT Sector: Includes telecommunication networks, submarines, communication towers, communication satellites, and ISPs (Internet Service Providers).

- Energy Sector: The energy sector includes the systems, networks, and stations that control the production and distribution of electricity, oil & gas, dam stations, and nuclear power plants.

- Transportation Sector: Includes air, land, sea, and River Nile transport. The transportation sector also covers all trains, metro control systems, centers & networks, sea and air navigation traffic networks.

- Information and Culture Sector: This includes networks, systems, information and broadcasting services. (Egypt National Cybersecurity Strategy, 2017)

By focusing on these critical sectors, the Cybersecurity strategy aims to prevent a total blackout of services in case of an attack.

4.3 Conclusion

The goal of this chapter was to identify areas of strength in other countries, in regard to cybersecurity. This will help us understand where Somalia lies in respect to other countries, as well as learn what key activities are crucial to an improved cybersecurity landscape in the country.

From the study above, we can see that the developed countries make cybersecurity a priority, involving all their citizens in this movement. This is also due to the fact that they are more connected to the Internet, especially due to the rise of Internet of Things, and thus are more at risk of an attack. We identified three main capacities of

focus by the developed world, that is, increased funding, dedicated cybersecurity agencies and the creation of an all-inclusive cybersecurity awareness culture.

The spending capabilities in terms of cybersecurity of the developed nations analysed were seen to be very high, unlike in the developing countries where the investment is very low. Both the developing and developed countries have cybersecurity agencies, with the developed countries being more mature and better staffed.

The cybersecurity agencies of the developed countries set up cybersecurity strategies for their countries, with full government backing. They also have clear and direct regulations guiding their activities with the institutions within the countries. These activities include mandatory reporting of incidents and strict measures directing corporations to protect private data. This is not yet in effect in many developing nations.

Developed countries understand that creating a good cybersecurity awareness culture involves encompassing the entire population. They create several campaigns and trainings to educate their general public about the dangers online. We see several developing countries starting to adopt this ideology with cybersecurity awareness activities being undertaken online such as National Cyber Security Awareness Month.

5. Cybersecurity landscape in Somalia

In order to understand the current level of cybersecurity awareness in Somalia, we must first analyse the level of maturity of the ICT infrastructure within the country. The growth of the ICT sector will help us understand how big the attack surface is within Somalia. We look at where Somalia is in terms of cybersecurity and what controls are in place. We then consider the threats facing Somalia and what routes it can take to solve these problems.

5.1 Overview of Somalia's ICT Infrastructure

In Somalia, however, there is apparently a healthy ICT infrastructure, which is mostly found in urban centers and particularly in Mogadishu, the capital city (Hare, 2007).

In recent years, Somalia has seen a growth in Internet users. Online users were at 1.63 million or 1.5% of the population in 2020 (Kemp, 2020). We are seeing a trend as growth on the internet within Somalia that has led to a very high rise in ICT usage within the country. ICT is the most active sector in Somalia's economy. It is one of the main segments of GDP per annum of the country (UNDP, 2012). Local companies have merged and developed the ICT sector (Hesse, 2010). ICT services are commonly and economically available to Somalis due to the rapid increase in local companies (Unwin, 2009). The ICT sector can also influence other sectors by boosting productivity and profitability and thus stimulating investment. This digital opportunity can help generate for the people, companies, and the country as a whole, influencing growth and well-being.

In January 2011, the Somali chapter of the Internet Society was established. Its goal is to promote the rapid spread of Internet and its technologies in the Somali Community. It also creates more awareness about internet security and cybersecurity by disseminating information to IT professionals within the country. It does this by embarking on campaigns like Safer Internet Day Somalia, where it shares information related to safe internet usage for educational, business and social activities. The Somalia ISOC chapter launched the Internet Governance Forum Somalia in November 2020. This forum assists the ICT sector by facilitating discussions and assisting exchange and sharing of ideas (Unwin, 2009).

The five-year '2019 - 2024, National ICT Policy and Strategy' has been introduced by the government to promote ICT in social and economic development (Immigration and Refugee Board of Canada, 2015). This policy intends to renovate the digital landscape and make society more knowledge based and inclusive. The layout of this policy is as follows:

- Increase the scope of e-commerce.
- Increase the role of online media in financial services.

- Spread digital literacy and R&D.
- E-governance in areas of health, agriculture, and infrastructure.
- Increase network coverage.
- Local hosting, domain names, cyber security and improving service quality.

After the National Communications Law was passed in 2017, the NCA (National Communications Agency) was established as the regulatory body to protect the communications sector within Somalia. They enable the government to obtain revenue by licensing spectrum to companies. They are also in the process of developing a number of regulations, for example, the Unified Licensing Framework (Lancaster, 2018).

As per the Somali Economic Forum, there are more than 20 active telecom companies in Somalia. The most popular ones include Hormuud, Golis, Telecom, Amtel, and Telesom. There are signs of entrepreneurship and innovation in the market, using technology and business acumen (Lancaster, 2018). Some examples are as follows:

- Better Business Solutions is a consultancy company that helps young entrepreneurs develop business plans, formulate market research, and manage funding.

- Guri Yagleel is also an online management program which aims to simplify access to rental and properties in the country for citizens.

- ePocket is an electronic payment system selected in the 2016 Innovate Accelerator programme. This application connects banks, which helps people all over the country to shop online, pay utility bills and school fees through the Internet.

- Mogadishu-based Hormuud telecom launched an Electronic Voucher Card Plus (EVC Plus). This application makes it easier to perform mobile money transfers and transactions.

5.2 Cybersecurity situation in Somalia

In Somalia, cybersecurity has become a nationwide concern after the widespread global use of the Internet. Many government operations and processes have become digitalised. Cybercriminals use cyberspace to target the private and public institution's confidential assets to interrupt the essential infrastructure, exfiltrate the citizens and governments data. These criminals have multiple motives, such as obtaining financial benefits or supplying intelligence information to adversaries. Currently, no clearly defined cybersecurity strategy that can protect against cyberattacks on a large scale. According to Kaspersky, Somalia is in the top 20 countries with the highest number of computers affected by malware (Kaspersky, 2020).

Another statistic shows that 80% of Somalia's cyber incidents are by hacking governmental emails and web applications. Hence, there is no detection mechanism that can be used to track the origin of the attacks. Hacking emails, personal computers and web applications are some of the significant cyberattacks in Somalia in the last ten years (Devi, 2017).

To protect against cyber incidents and improve the country's security, major strategic and administrative decisions are required to be taken, including implementing a security awareness framework and instituting a national CERT (computer emergency response team). New initiatives and networks will be required, including networks between the police and government agencies, networks between policy and private institutions, and networks between research institutions and private organisations (Broadhurst, 2006).

At present, Somalia deficiencies a national cybersecurity strategy and directives, including cybersecurity standards, frameworks, policies, and awareness programs. Somalia is categorized as one of the worst cyber secure countries, indicating a vast gap between international standards and a national cybersecurity plan. Somalia does not have a specific educational and training programs center for cybersecurity in the country. In addition to that, there is no a single platform where Somalia people can get an awareness of cybersecurity threats (Sambuli et al., 2015). There is a lack of

well-trained cybersecurity professionals and the level of understanding of cybersecurity issues among law enforcement agents and the courts of law are currently very low.

On a strategic level within an organisation, cybersecurity as an activity of protecting information, polices should be aligned with cyber ethics, cybersecurity and safety measures. As an organisation and as a function, cybersecurity is helping and adding value to a business. The protected environment of a business with a detection and response programme in place will not only diminish restrictive preventative controls, but it will also reduce the shadow of information technology, which will enable organisations to increase their overall productivity (Brotherston et al., 2017).

Similarly, a country should develop strategic objectives for protecting its citizens and critical IT infrastructure on a national level. It should form a dedicated department responsible for developing and maintaining requisite cybersecurity policies and strategies. On this note, Somalia has the NCA, which is the official point of contact for SMEs, government agencies, ICT solutions, Internet Service Providers (ISPs), citizens, and critical infrastructure providers (NCA, 2018). It has a comprehensive national level mandate including raising cybersecurity awareness across the country and developing national cybersecurity strategies. Other objectives include:

- Administering the responsibilities of SomCERT/CC
- Identify, prevent, and respond to adverse cyber incidents, including offering advice and developing necessary regulations
- Lead and coordinate the response efforts to crisis situations as a result of malicious cyber incidents
- Review and certify cybersecurity processes applied to protect information technology systems and products
- Raise national cybersecurity awareness by encouraging critical infrastructure and public services operators to understand and adhere to cybersecurity requirements.

With the creation of the National Communications Agency, a cybersecurity department was created to protect, monitor and secure Somalia’s cyber space and

valuable cyber assets. All cybersecurity incidents are to be reported to the NCA though there are no laws mandating this (NCA, 2018). In May 2019, a Computer Emergency Response Team was established under the cybersecurity department of the National Communications Agency. Its main objective is to create a safer, stronger internet for all Somalis. According to the official website (Som-CERT, 2018). They intend to provide following:

- Supplying intrusion detection and prevention to government organizations.
- Developing cybersecurity awareness information to government agencies and critical infrastructure owners.
- Countering to cybersecurity incidents within Somalia.
- Cooperating with other CERTs around the world to enhance Somalia's cybersecurity posture.

The Somalia CERT provides alerts and instructions on their website; however, they do not have any cybersecurity awareness plan in order to reach a greater amount of the population. They are also not on any social media platforms thus missing an important outlet to reach a greater amount of people.

The CERT team is a member of the OIC-CERT (Organisation of the Islam Countries – CERT) and Africa-CERT vastly improving its ability to cooperate with the various countries attached to these bodies. It should however also work towards joining several other international security teams like FIRST (Forum of Incident Response and Security Teams). This will provide capacity building opportunities, increased collaboration with other CERTs, as well as access to a plethora of information that can be used to grow Somalia CERT's response capabilities (Som-CERT, 2018).

5.3 Challenges facing Somalia

An externally focused, transparent and relatively unregulated economy has flourished amid decades of conflict (Little, 2003). Enterprising firms have provided Somalis with ways of sending and receiving capital. There is also an increased activity by the Somalia diaspora in increasing investments within the country. This has enabled telecommunications companies, as well as the ICT sector to operate successfully.

Cyberattacks in Somalia can be due to vulnerable systems and a lack of cybersecurity standards. Pirated software products are very common and inexpensive. This security software is unable to be upgraded from the manufacturers' versions, hence spreading malware (Symantec, 2016). The growth provides increased access to cyberspace, without adequate security measures. A solid regulatory framework makes it possible to regulate authority, punish crimes, and control implementations in cyberspace. Lack of this would negatively impact the use of the Internet and increase the rate of cybercrime within Somalia.

In Somalia, financial crimes are popular. Due to the lack of formal regulatory and banking structures and complex relationships between courts, the government is unable to regulate and resolve money conflicts; scams, inaccurate transactions or disputes over the volume of the transfer (Bashir, 2019). The judiciary system within the country should be vastly improved in order to deal with cybercrime and electronic evidence. The lack of knowledge and skills among prosecutors and in particular judges are a key issue here and specialized training should be provided to them.

Somalia's weak ICT infrastructure results in security breaches of their private and public institution's sensitive data. It indicates that the agencies in the country required to respond and resolve cyber related issues are not yet mature enough to do so. Moreover, poor and flawed rules and law enforcement are another concern in the country. Despite the fact that telecommunication companies have expanded rapidly, and the industry has flourished, even without a state regulatory structure, this has helped Somalia to stabilise as well as providing fertile ground for cybercrime activities (Stremlau, 2012).

Another challenge faced by ICT and cyberspace in Somalia is a fundamentalist group called Al-Shabab. Rules and regulations have become more difficult to enforce in the Al-Shabaab-controlled regions, which have heavily limited the use of ICTs and prohibited Internet usage, calling it un-Islamic. However, the party makes use of social media to advance its cause, posing possible risks to its neighbors. Al-Shabaab has presented a new collection of obstacles and problems for the country. Anti-

terrorism efforts have taken seriously the use of new technologies and the potential threat of cyber-attacks (Sambuli et al., 2015).

There is a lack of funding provided to cybersecurity within Somalia. This diminishes the capacity of the citizens and institutions to monitor and follow cybersecurity within the country. In many African countries, cybersecurity is perceived as a luxury, not a requirement. Its significance has still not been properly considered or accepted. The budget for cybersecurity is estimated to be less than 1% in many organisations (Kshetri, 2013). Cyber threat detection and incident response capabilities should be enhanced and these require input of resources.

Another concern is the absence of abilities among Internet users to defend themselves from cyber-attacks. Most Internet users are novice and are not technically competent. There is an extreme shortage of a skilled workforce in the country. Many organisations, specifically government agencies, lack expert IT personnel, which leads the organisations to become more vulnerable to cybercrime (Kshetri, 2019). There is a need for awareness and technical education in the field of cybersecurity. Capacity building campains should be undertaken to increase the capabilities of the citizens to improve the cyberspace within Somalia.

With the organizations dealing with cybersecurity in Somalia in their creation stages, it is possible that there is no robust capability to deal with cybersecurity. Cybersecurity is not a phase but rather a continuous process. Therefore, it is not only the matter of passing legislation but parliamentarians, attorneys, the courts, intelligence and military, civil society, media, youth and the public should all be active in efforts to resolve cybersecurity at the utmost possible opportunity. It is necessary to engage all stakeholders to understand the concerns and processes involved (UNECA, 2014).

In addition, all cybercrimes involving digital technologies should be covered, and computer networks should also demand a standard of emerging networks such as police and government department networks, police-private networks, and foreign-police networks (Broadhurst, 2006).

5.4 Towards cybersecurity Awareness

In this case, information systems (hardware and software) require suitable technological and practical security measures. The provided firewalls, antivirus software and other technological solutions for safeguarding personal data and computer networks are indispensable but not enough to ensure security (Allan et al., 2013). It is a priority to build a cyber-infrastructure; however, it is equally important that training is provided to function efficiently and effectively within the infrastructure (Abhishek et al., 2015). There are five primary benefits of implementing cybersecurity training and awareness programs in an organization:

- Training reduces costly mistakes: Careless mistakes when using accessing and interacting with critical IT assets account for the highest percentage of cyberattacks. Errors, such as clicking on phishing emails, can expose a company at risk of being attacked, resulting in data breaches and exfiltration. Executing a training program empowers system users to be more alert since it imparts relevant skills and best cybersecurity practices.

- Training and awareness enhance cybersecurity: With employees being aware of best cybersecurity practices, such as password protection, information backup operations, and multi-factor authentication, an organization can realize a more effective cybersecurity state.

- Continuous training expands security consistency: Different organizations implement differing awareness and training life-cycle. However, exposing system users to continuous training programs ensures they remain consistent in demonstrating high levels of cybersecurity knowledge and awareness. Thus, a company can protect itself from modern threats and attacks.

- Increased confidence: Cyber-attacks advance everyday as adversaries leverage emerging technologies to evade detection and increase the rate of successful attacks. However, a cybersecurity mindfulness preparing program enlightens everyone regarding cyber threats and how to be cautious when

using digital technologies in an online world, enhancing occupation fulfilment among users.

Hybrid strategies are sought in Somalia in the absence of a functional state that incorporates traditional approaches and emerging technology to provide individuals with some degree of certainty using critical resources such as local and international mobile payments (Sambuli et al., 2015). While Somalia's Internet access and use is increasing very gradually, the country has a post office and telecoms ministry to manage the ICT (Information and Communication Technologies) market. Much of the sector remains unregulated. Local authorities in certain regions make the rules on what residents can or may not do with ICT (NCA, 2018). There has however been no study done to understand the level of cybersecurity awareness within Somalia. This should be the starting point for the organizations responsible for this activity, namely, the NCA, the Somalia CERT and the Somalia chapter of the Internet Society.

Despite starting a Somalia CERT, there is little to no collaboration with the private sector for cybersecurity issues. This creates a gap between the private and the public sector. There is a need for cooperation and coordination between the two sectors. Although, the government has started prioritising the cybersecurity sector to regulate data protection. The core challenge for the government of Somalia is the lack of public awareness. Also, there is no national cybersecurity awareness campaign. The government has considered initiating one, but the plan is not yet wholly executed. The Somalian government's primary responsibility in the coming years is not only to eliminate the threat to national cybersecurity but also to implement national strategies and regulations to control and monitor these processes effectively (Symantec, 2016).

Our assessment shows that cybersecurity awareness should be focused on all areas of society: the government to create the regulations, the judiciary to enforce them, the education sector to teach them and the society to abide by them. Understanding what cybersecurity incidents that affecting these sectors is paramount.

6 Survey results and analysis

This chapter will provide an evaluation of cybersecurity development in different sectors of Somalia. The top sectors within a country include: banking and finance, central government, communications, energy, health, and transportation. We shall be looking at three of these sectors, namely, the bank institutions, telecom companies and government institutions. We shall also be gauging the general public.

We were not able to look at the energy, health and transportation sectors due to time constraints, as well as the fact that these sectors are not as developed as the others within Somalia. It is very important to note that attacks on one sector of a country can have a ripple effect and affect other sectors. An attack on a country's telecommunications, for example, may disrupt electronic payments in the banking sector. Therefore, we looked at the most predominant sectors in Somalia, in terms of number of users and ICT integration.

The first survey shall look at the general public. We cannot analyse the level of cybersecurity in Somalia without first looking at the people of Somalia. With more and more people connecting to the Internet, the possibility of hackers targeting individuals vastly increases. By starting the survey with the general public, we can understand the ripple effect that spreads out to the institutions. For criminals, targeting people makes sense. It's faster, easier and cheaper than targeting systems.

Cybercriminals are attacking smaller businesses and home users as they usually have less technical knowledge and equipment to ward off their attacks. These attacks can be very damaging to individuals as they often don't have the resources to easily recover. The advent of social media also helped increase the attack surface, introducing new risk. People usually act in two-capacities, both as users of the services of information technology and as employees. This makes them very essential, since their behaviour with technologies can facilitate or prevent the success of a cyber-incident.

The Banking and finance sector was chosen because it is usually the one most affected by cyberattacks. The majority of cybercrimes in the world involve a form of monetary gain for the attackers. Thus, it is much more noteworthy for cybercriminals

to attack a bank than to hack, let's say, a defense plant (Sachkov, 2017). Most bad actors are motivated by money and so it serves to inform that banks would be very big targets, thus banks contain a very higher cyber risks as compared towards other organisations.

Telecommunication service providers are a huge bull's eye for cyber attackers as they operate critical infrastructure responsible for communication, as well as having a collective point for sensitive information. A denial-of-service attack would thus be very extensive with all communications coming to a standstill. They also collect and store a large amount of information on their customers, such as, id information, addresses, connection and financial data. This sensitive data can be used to conduct identity theft, blackmail or used to launch further attacks through social engineering. With a big number of companies currently providing telecommunications services in Somalia, this was seen as a very key sector to investigate and identify the current state of cybersecurity within these sectors.

Government is a likely target for cybercriminals. They usually possess a wealth of personal information like date of births, addresses, national identity numbers, that is very juicy to attackers. Attackers also target the government in order to block critical services and operations provided by the government or administration or be the subject of propaganda attacks. Attacks targeting government websites have been seen in plenty within Somalia.

These attacks are compounded by the fact that many government entities still operate legacy systems with obsolete or limited support. This makes them high risk especially when little effort is provided to cybersecurity. Therefore, it is imperative government assumes a headship role in promoting a safe cyberspace that creates confidence in businesses and citizens as whole facilitating social, economic and industrial growth.

Hence, the chapter is divided into four sections: survey for public awareness, survey for banking institutions, telecommunication service provider’s survey and government sectors survey. The survey was created and distributed online using

Google forms amongst the individuals of these stakeholders through social networking and email platforms.

6.1 Public awareness survey

We conducted a public awareness survey to evaluate the cyber awareness level of random public members not associated with a specific organization. The questionnaire consisted of seven questions designed to understand Somalis' use of the Internet and test familiarity of a number of cybersecurity terms and habits. The questions deal with issues that users face, as well as basic cybersecurity behaviours that users should be doing on a daily basis.

We received 84 responses from 6 cities within Somalia, namely, Mogadishu, Hargeisa, Garowe, Kismayo, Merca and Borama. These cities were selected as they are all in different regions in Somalia and have big populations. This would give us a deeper view on the situation within the entire country. The participants also needed to use the internet to complete the study and hence were required to have an internet connection.

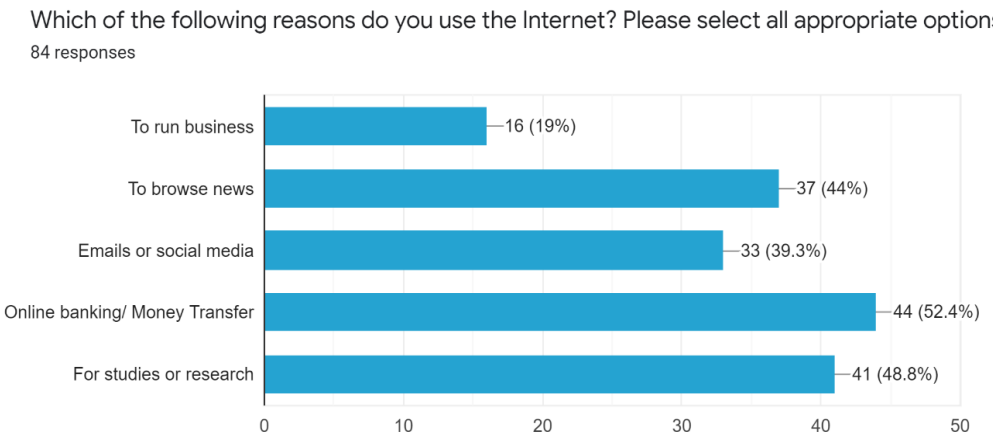


Figure 1: Reasons for internet usage in general public

Finding out the main use of the internet for the general public would help us understand what is most at risk in case of a cyber-attack. The main reason why most people use the internet in Somalia is to access online banking/money transfer services, with 52.4% of the survey participants indicating so. Also, 48.8% of the

respondents stated they primarily use the internet for study and research. Furthermore, 44% of the people participating in the survey indicated that they use the internet to browse current news. However, vital reasons for using the internet like running a business had least responses with 19%, and email or social media had the low responses with 39.3%. The extensiveness of digital banking in Somalia is proof that the Web has gained enough credibility to make ordinary people feel comfortable using it. This illustrates the depth at which general public are at a high risk of financial loss.

From the survey's output, it is clear that cybersecurity awareness efforts should focus on educating individuals on how to protect themselves from attacks targeting online banking/money transfer, such as phishing and identity theft. Moreover, performing the survey was advantageous since it established that studies and research account for the second-highest number of people accessing the internet. This shows that students are amongst the most vulnerable and require specialized awareness training. Social media and email are important methods used to deliver phishing links and harmful programs thus creating awareness on how to remain safe when accessing social media or email services is essential.

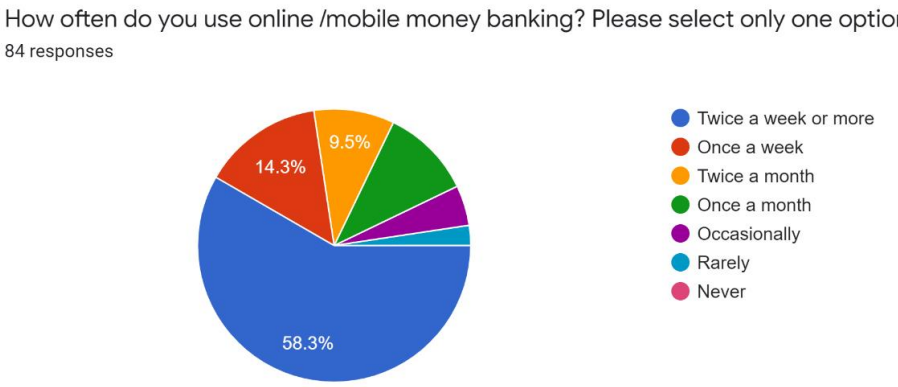


Figure 2: Frequency of online banking/mobile money banking usage

There is a notable trend between this survey question and the previous one since it indicates a high frequency of online banking. This will help us gauge the reliance on online banking/ mobile money. In the bar chart above, 84 participants, 58.3%, use online banking/mobile transfer at least two times a week. Also, the number of

people using online banking once a week is relatively high, where 14.3% of the respondents stated they use the service once a week. As indicated in the diagram, the frequency of using online banking decreases with time, meaning that shorter periods record a higher frequency of usage compared to longer periods.

This has shown us that the majority of people do not just use online banking/mobile money banking for business purposes, but for day-to-day activities like buying groceries and paying utilities. The implication of the above survey output is relevant authorities, and regulatory bodies require to pay more attention to creating awareness among online banking users. Since cyber adversaries devise complex methods for compromising online banking users, there should be policies subjecting users to frequent awareness programs. For example, raising awareness once a month should be adequate to enlighten users regarding recent online banking threats and how to remain protected.

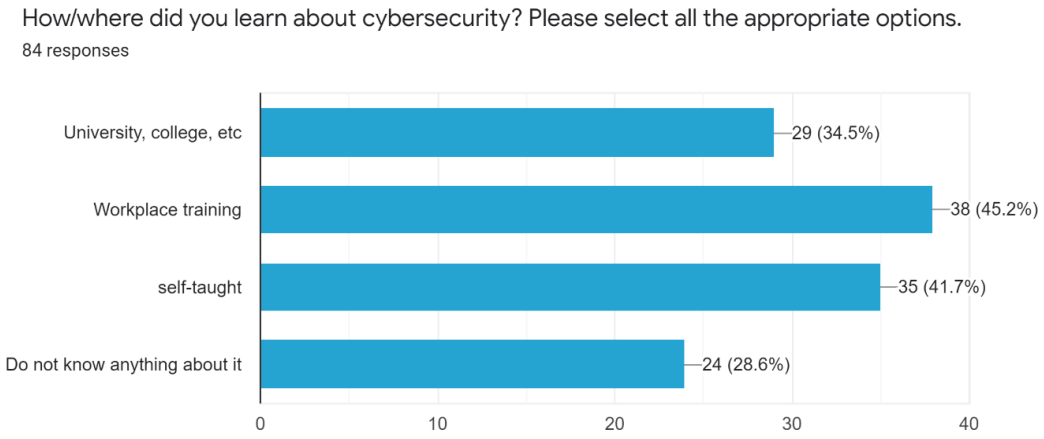


Figure 3: Sources of information on cyber security

Cyber awareness is a critical requirement for everyone since the current threat landscape is highly dynamic and evolving every day. However, it was surprising when this survey question showed that little effort is used to raise cyber awareness in Somalia. The number of people who learned information security through self-learning accounted for 41.7%. In addition, it was worrying about finding out that 28.6% of the randomly selected participants don't have any idea what information security is. On the bright side, 45.2% of the respondents acquired information

security awareness from workplace training, while an additional 34.5% learnt cybersecurity in college or university.

The questions' primary advantage is it identified a considerable gap in public cybersecurity/information security awareness in Somalia. It is critical to raise the awareness level among individuals through robust information security training campaigns. The majority of participants learnt about cybersecurity from workplace training as institutions have the most to lose in case of a breach. It is therefore very crucial for them to ensure that every employee possesses skills for secure information usage to preserve its confidentiality, integrity, and availability. Although a large amount of people surveyed acquired cybersecurity awareness through self-learning, it may not be enough since they require a competent professional or body updated with current best practices for deterring modern cybersecurity threats.

We have identified a large gap in the education system specifically universities and colleges, in educating the general public on cyber security, with just a third learning about cybersecurity. With many students using the internet for research purposes, there is a need for cybersecurity to be taught at schools. The use of ICT in the workplace has vastly increased and many employers require employees to have a working knowledge of these technologies. Adding cybersecurity awareness training to the syllabus can be an incentive to both the school and the student as it greatly enhances the possibility of getting a job.

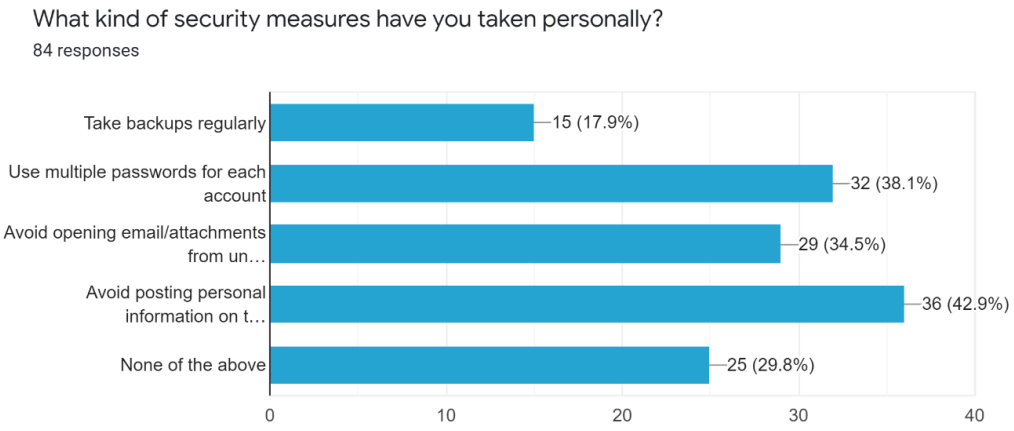


Figure 4: Individual security measures taken

Personal cybersecurity preparedness and protection should be an individual responsibility in the currently digitized world. Despite this, 29.8% of the people who participated in this survey admitted that they hadn't implemented any cyber protection measures. However, 38.1% use different passwords to secure their accounts, representing the highest number of people using passwords as the preferred security method. 34.5% of the respondents indicated they don't open email or attachments sent from unknown sources as a security measure while 42.9% avoid posting personal information on social media platforms. The least taken measure with 17.9% of the respondents in regular use of backups.

The most notable output from the survey is that nearly one third of the participants don't apply any security measures for their own protection. It is a clear indication that they lack awareness of the essence of maintaining healthy security practices on a personal level. Another crucial trend noted in the survey is the majority of users prefer password protection for their different accounts. In this case, they need to be aware of how to reinforce password management practices by augmenting it with other practices like multi-factor authentication. With the low number of individuals performing backups, it is important for cyber awareness campaigns to sensitize the public on the best practices for maintaining backups and why it is essential. This illustrates a very high risk of data loss in case of malware or malice.

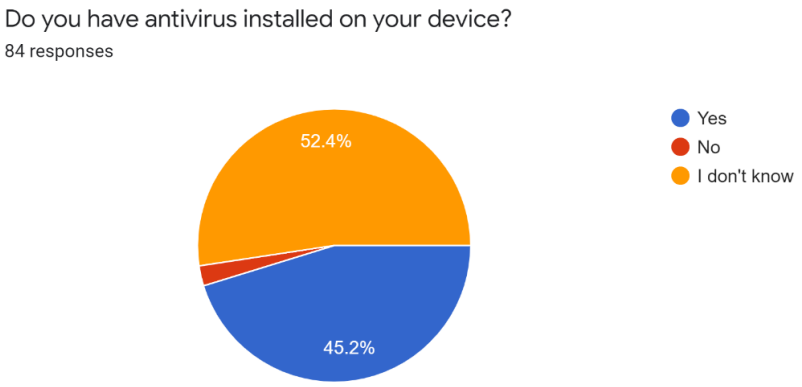


Figure 5: Prevalence of anti-virus on user devices

Antivirus solutions are helpful in protecting devices from malicious network traffic and harmful programs. From the responses given to the survey question, 52.4% of

the participants do not know whether antivirus was installed on their devices. 45.2% of the participants have installed antivirus, while only 2% have not installed antivirus on their devices. This provides some comfort as the about half of the participants have antivirus software installed.

The fact that the majority of participants do not know whether they have antivirus software installed on their devices is very worrying. This could be attributed to the fact that many people use their mobile devices for a lot of the online activity and there is little awareness spread about protecting mobile devices. This is very dangerous as there is a rise of malware targeting mobile devices, especially Android devices as it open-source software. Android allows developers to upload apps to the google play store and as such are at higher risk for malicious applications. Antivirus solutions can help identify these malicious applications, as well as protecting from malware downloaded through web browsing.

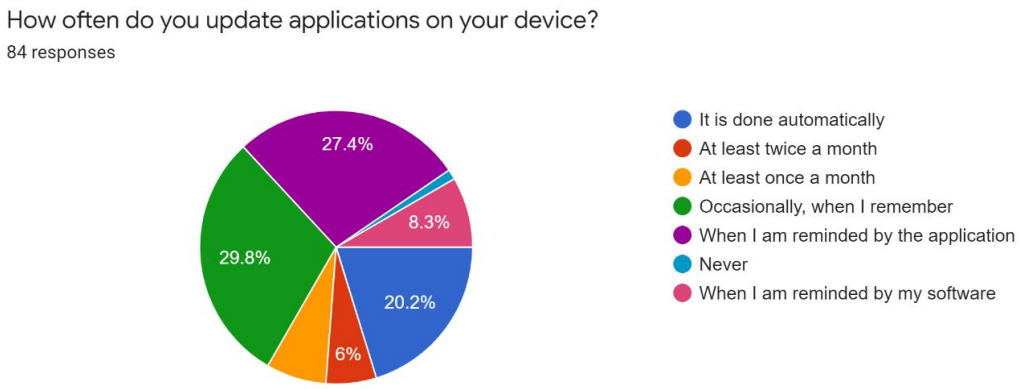


Figure 6: Frequency of application updates on user devices

Software updates are very important as they usually fix security holes found in applications. These holes can be used by attackers to gain access to a person's device. Updating ones' devices can help keep attackers out. This survey question's importance is to evaluate if the public users in Somalia are aware of the need to update applications frequently. From the results, 29.8% stated they occasionally update when they remember. However, 20.2% of the respondents have set it to update automatically, which is a recommended security practice. There was also

some frequency in the survey results, where 6% stated they update it at least twice a month, and 27.4% update occasionally when reminded by the application.

The survey results indicate a lack of awareness in Somalia regarding the essence of updating application software frequently. Most of the respondents only update if the application reminds, which places their devices at risk of compromise. Software vulnerabilities are a great deal and many more keep on being discovered. A cybersecurity awareness campaign is necessary to enlighten users on how to update their applications automatically to remain protected.

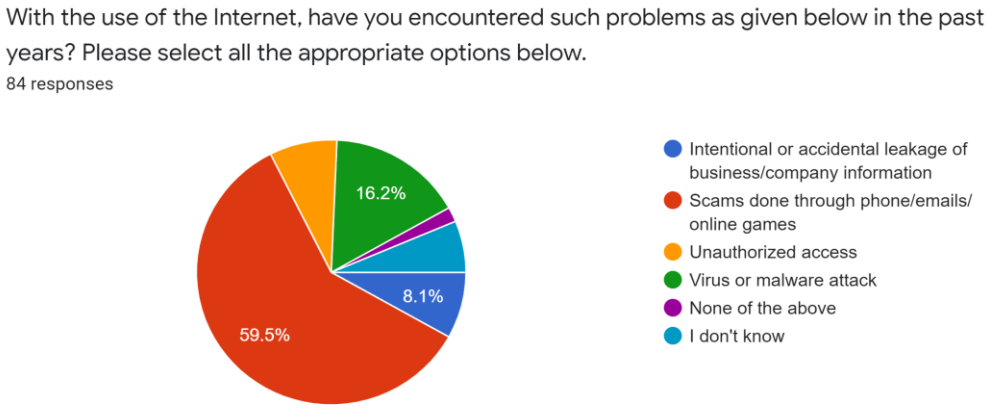


Figure 7: Problems encountered from Internet usage in the past two years

Understanding the most common security incidents faced by the general public can help us save time and effort in cybersecurity awareness campaigns. By looking at the information above, we can reduce more than half the incidents by just focusing on one cybersecurity attack vector. Most participants in this survey (59.5%) stated that they had encountered scams done through emails, phones, and online games. However, 16.2% selected virus or malware attacks as the security issues they have experienced when using the internet. An additional 8.1% chose intentional or accidental leakage of company information. Instances of unauthorized access were also common among the respondents, while a small number of people indicated they don't know or none of the options provided in the survey.

This survey output shows that a lack of training exposes many Somali people to online scams. The most significant percentage consists of individuals who have faced

online scams in the past two years. Therefore, cybersecurity awareness programs need to address this challenge and equip the necessary skills for avoiding scams and social engineering attacks. Moreover, antivirus and malware attacks were also common, which could be linked to the lack of awareness on updating antivirus software. Somali companies should also implement measures for preventing intentional or accidental leakage of sensitive business information and train employees on best practices for preserving data integrity, availability, and confidentiality.

6.2 Survey on bank institutions

This survey contained 12 questions drawing 51 responses from participants in the banking sector in Somalia. The participants included managers, staff members, and employees drawn from the top four banks in Somalia. The selected banks are located in three different cities to ensure the results reflect other regions' cybersecurity awareness levels. The cities are Mogadishu, Garowe, and Hargeisa.

The questions in this survey aimed to understand:

- the current controls being deployed by banking institutions and how they are managed.
- how they secure different kinds of data.
- gaps in their day-to-day activities that can lead to a cybersecurity incident.
- the most common cybersecurity incidents recorded.
- The relationships with third party providers.

The results and survey analysis are as follows:

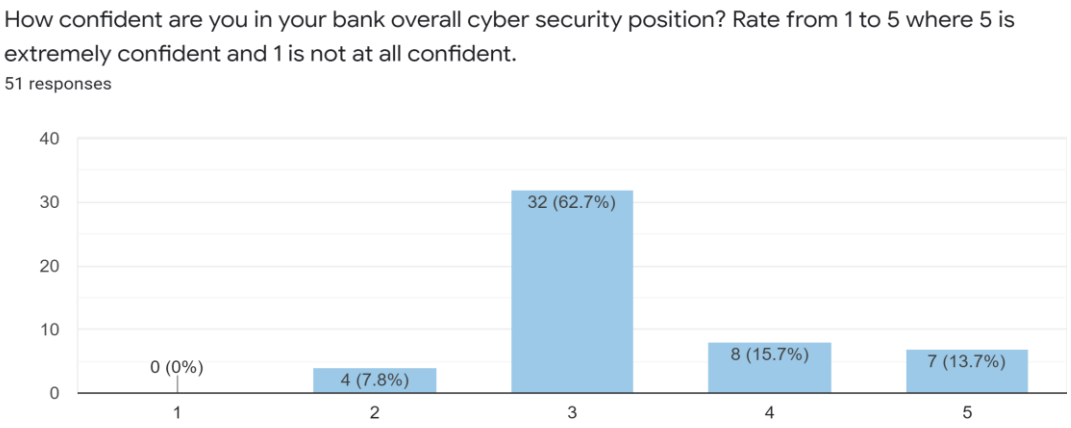


Figure 8: Degree of confidence in the banks' overall cyber security position

According to the respondents who participated in this survey question, 15.7% said they have confidence in their banks' cybersecurity position, while 13.7% said they are extremely confident. Nevertheless, 62.7% of the participants were unsure if they were confident about their banks' current cybersecurity position. On the other hand, 7.8% of the respondents said they are not confident in their banks' cybersecurity.

The survey results show that a large number of participants are uncertain if they can trust their banks' cybersecurity processes. It is an indication that bank organizations in Somalia may not be implementing some required cybersecurity standards or controls, which may cause doubts about their effectiveness. However, the encouraging news is that at least 15 respondents showed confidence in their banks' cybersecurity practices. The benefit of the survey output is it reveals that Somali banks have an average cybersecurity awareness level. It further showed that bank institutions need to prioritize cybersecurity controls to acquire all involved parties' trust and confidence.

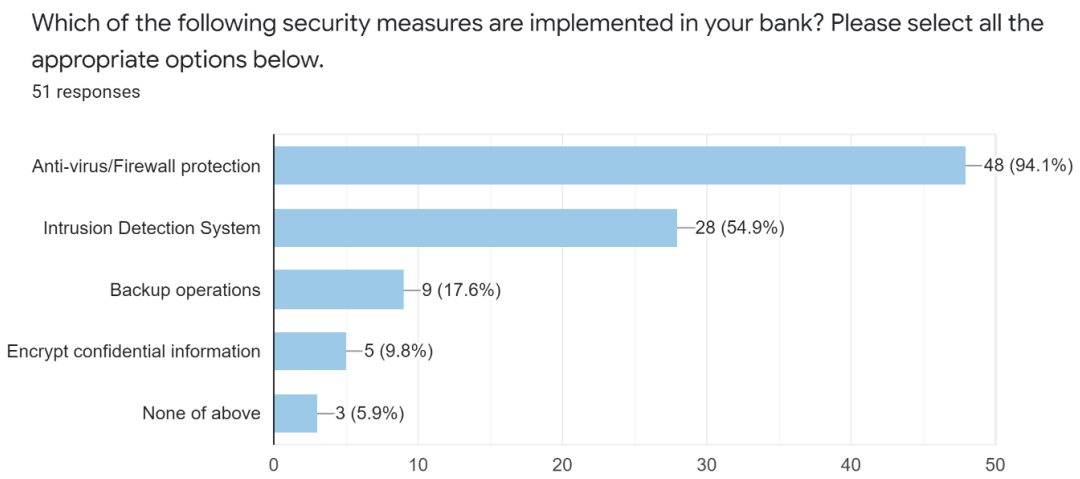


Figure 9: Security measures implemented in the bank

The responses to this survey question indicate that 94.1% of banks prefer using antivirus/firewall solutions. In addition, 54.9% of the respondents indicated that their bank institutions had deployed intrusion detection systems. On the same survey, 17.6% of the participants agreed that their bank organizations observe system/info backup operations as a security measure. It was, however, concerning that a small number of respondents chose encryption of confidential information as having been implemented in their banks. 5% of the participants stated that they were using none of the above-mentioned security measures.

The survey output reveals exciting facts about cybersecurity implementations in Somali banks. Antivirus and firewall appliances and deployments are crucial cybersecurity measures that enable the detection and prevention of malware attacks and filtering malicious network traffic. As such, this explains why most participants indicated that they are the most used network security measures in their bank entities. However, the survey shows that some organizations are yet to implement the most fundamental network security measures, which can expose banks to internal and external breaches.

Intrusion detection systems assist in detecting and stopping attempted intrusions that may lead to a data breach. Besides, a low number of organizations perform a backup and implement encryption measures, despite being vital cybersecurity requirements in banks. Furthermore, encryption technologies are helpful in

preventing unauthorized access to confidential customer or bank information. Moreover, frequent backups prevent data loss or corruption during a breach incident. With the rise of ransomware, banking institutions should make this a priority.

We also realized a large amount of the organisations are not encrypting their confidential information. This entails that their data can be disclosed to unauthorized individuals and these users can then modify this data. This very disturbing as banks hold a lot of personal information on customers and employees.

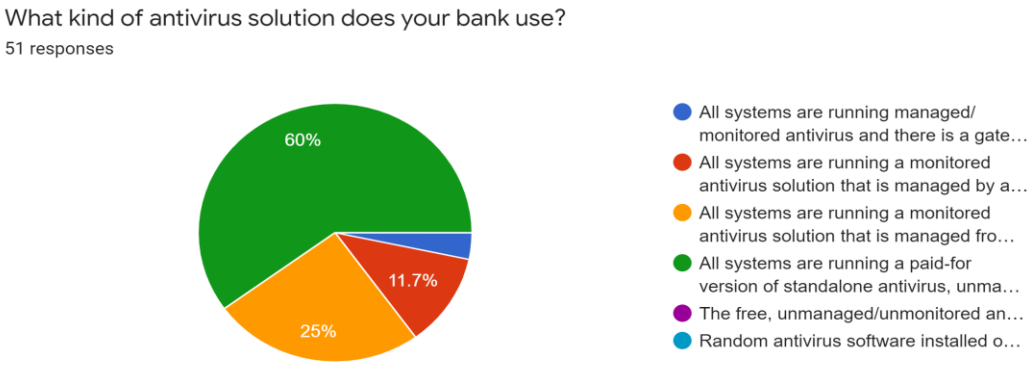


Figure 10: Types of Antivirus solutions used

It is not enough having and installing an antivirus, it has to be monitored constantly for threats. This question aimed to identify if the antivirus solutions are paid, managed or have a UTM solution. From the pie chart, 60% show that their organizations run a paid-for standalone antivirus version unmanaged and unmonitored. A further 25% revealed that all systems in their organizations running monitored antivirus solutions managed from the organizations' central servers. The survey also revealed that systems deployed in 11.7% of the respondents' organizations run a monitored antivirus solution managed by a third-party IT service provider. Only a small number of the participants indicated that their systems run managed/monitored antivirus with a gateway UTM solution.

The benefit of the survey output is, it clearly indicates that majority of bank organizations in Somalia use paid-for standalone antivirus solution that is unmonitored and unmanaged. The implication of this practice is that the standalone

antivirus versions may detect some malware and virus infections, but since no one is monitoring, no action is taken, thus exposing critical data and systems to avoidable attacks. While 25% of the participants stated that all systems run a monitored antivirus product managed on a central server, it is recommended to use one run by an external third-party provider. Therefore, cybersecurity awareness campaigns in Somalia should focus on creating more awareness on the benefits of using antivirus/firewall solutions with gateway UTM solutions managed by a third-party.

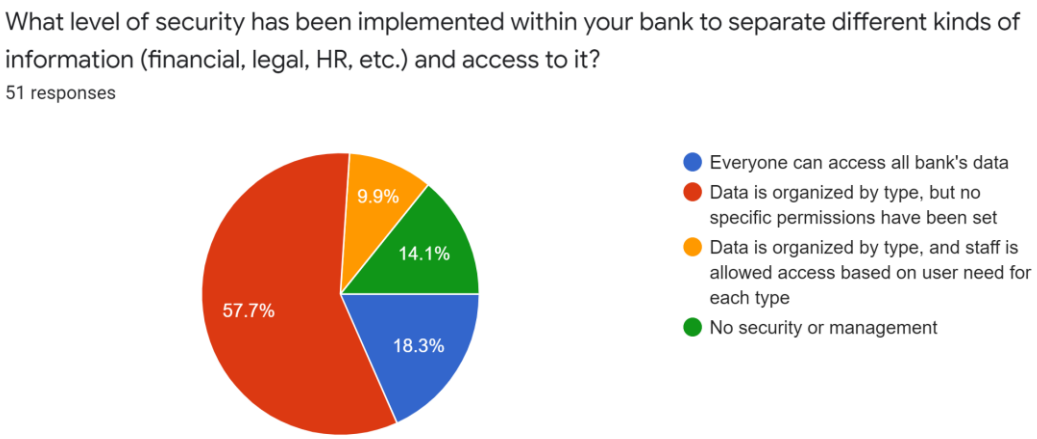


Figure 11: Level of security implementations for data within the bank

Access control is very vital in data security. We have to test a user to ensure they are allowed to access the data. This survey question checks to see if banks are implementing any authorization techniques to determine if a user is approved to access a specific set of resources and data.

It was discovered that most bank entities in Somalia have inadequate information security awareness and procedures. At least 57.7% of the responses indicated that banks categorize information according to type but do not implement special permissions for accessing it. Additionally, 9.9% of the participants stated that other than classifying data according to type, their bank organizations set specific permissions for accessing the data. However, a worrying trend identified in the survey is 18.3% of the participants indicated that their banks provide access permissions to all staff members irrespective of their roles, and 14.1% of the

participants said that their banks are yet to implement an information security management policy.

The survey output has been beneficial since it indicates the need to create information security awareness campaigns in Somalia's banking community. The awareness campaigns need to enlighten bank organizations on the essence of deploying sufficient access control measures, such as specific privileges for accessing data stored according to the type or categorized based on employee roles.

The awareness should further touch on the different access control methods for protecting unauthorized access to sensitive user information. Inadequate access controls expose bank organizations to multiple cyber threats, including data breaches, unauthorized access or modification of customer data, and insider threats. With Somalia having no data protection laws, the banks must take it upon themselves to impose these controls in order to protect their valuable information.

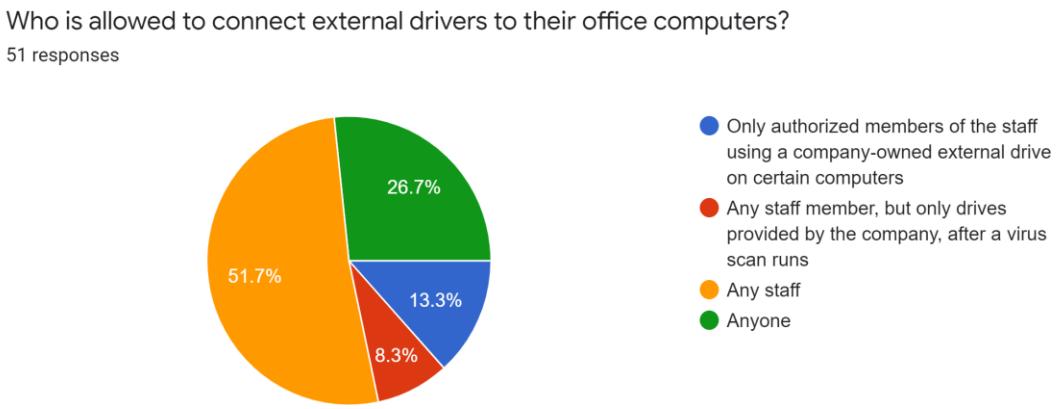


Figure 12: External drivers procedures for office computers

Connecting external drives in banks' systems can cause information theft, malware infection, and intrusions to secure networks and, therefore, a risky cybersecurity practice. Despite this, the pie chart above shows 51.7% of responses indicate that their organizations allow any staff to connect external drives to office computers. It also gets worse as 26.7% revealed that anyone could connect external drives to office computers.

However, it was impressive to note that 13.3% of the survey participants stated that their organizations only allowed authorized staff members to connect company-issued external drives on specific computers. Another notable statistic is that 8.3% of the participants said any staff member could connect, but only company-issued external drivers and must first scan them using antivirus software before connecting.

The primary issue identified from the survey is the huge number of bank organizations that permit anyone to connect an external drive, with 51.7% indicating so. However, adopting such a policy is ill-advised since it can expose a bank to avoidable security risks, including data exfiltration, insider threats, and easy introduction of malware using infected drives. As such, a cyber-awareness campaign on the use of external drives targeting the banking sector should be done to enlighten all organizations on the need to enforce policies governing the use of external drives on office computers.

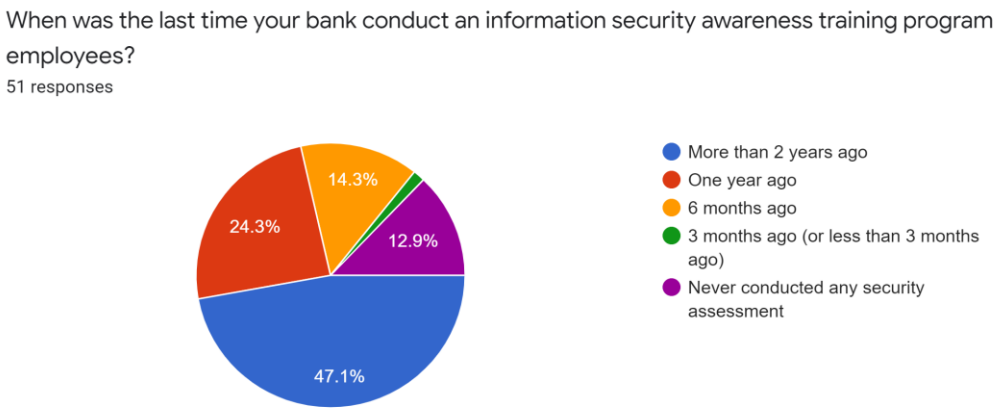


Figure 13: Regularity of employee information security awareness training in banks

Performing repeated information security awareness training campaigns provides employees with the skills required to identify and manage modern cybersecurity threats. The cybersecurity landscape is ever changing with attackers developing new methods at a very high rate. There is therefore a need to understand how often banks embark on cybersecurity awareness training campaigns. The banking sector's preferred awareness training frequency for starter training courses is quarterly (every three months). From the pie chart above, 47.1% of the respondents indicated

that their organizations performed information security awareness training more than two years ago, and 24.3% stated more than one year ago.

Furthermore, 14.3% selected the last six months as when their banks performed security awareness training. However, 12.9% revealed that their organizations have never conducted an information security training and awareness program. The green pie shows that a very small number of the participants stated that their banks performed an awareness campaign within the last three months.

The advantage of carrying out the survey is that 12.9% of banks in Somalia urgently require implementing information security awareness programs for their employees. Numerous researchers show that poorly trained employees are the highest risks to organizational security since attackers target vulnerable human elements the most.

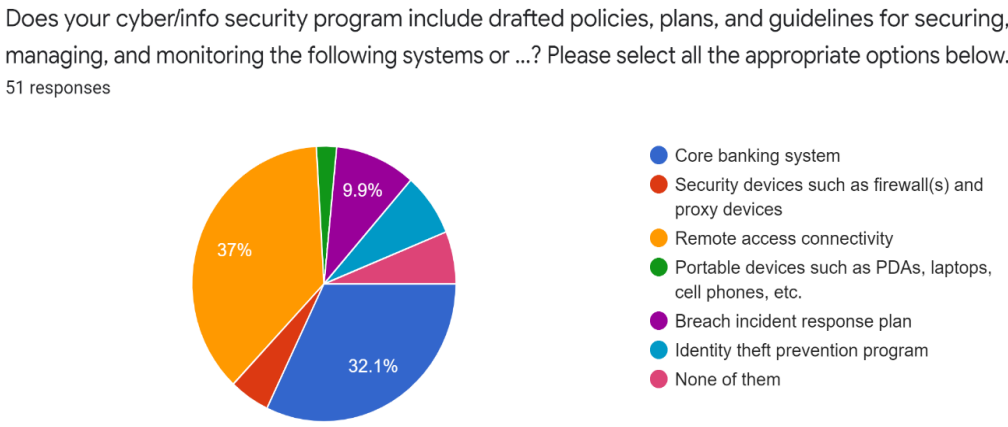


Figure 14: Available information security programs for monitoring systems in banks

The pie chart above shows that the information security programs of 37% of the respondents contain drafted policies, plans and guidelines for securing remote access connectivity. Also, 32.1% of the survey participants stated that their information security programs include written procedures for protecting the core banking system. Besides, 9.9% of the survey results show that they have a breach response plan in their information security programs. A small number of the respondents also indicated they have an identity theft prevention program in their information security policies. The green pie and red pie denote organizations with written

procedures for securing portable devices, such as PDAs, laptops, and cellphones, and security devices, such as firewalls and proxy devices.

The primary benefit of carrying out this survey is that it revealed a lack of awareness among bank organizations in developing and maintaining written information security policies and programs. The written policy with the highest responses is remote access connectivity with 37%. Written security procedures for securing essential devices contain a documented set of minimum-security requirements to observe for all users. With cyber-attacks targeting the banking sector more than other industries, it is vital to raise awareness on developing and maintaining written information security procedures to ensure all users observe the same cybersecurity standards when using specific devices.

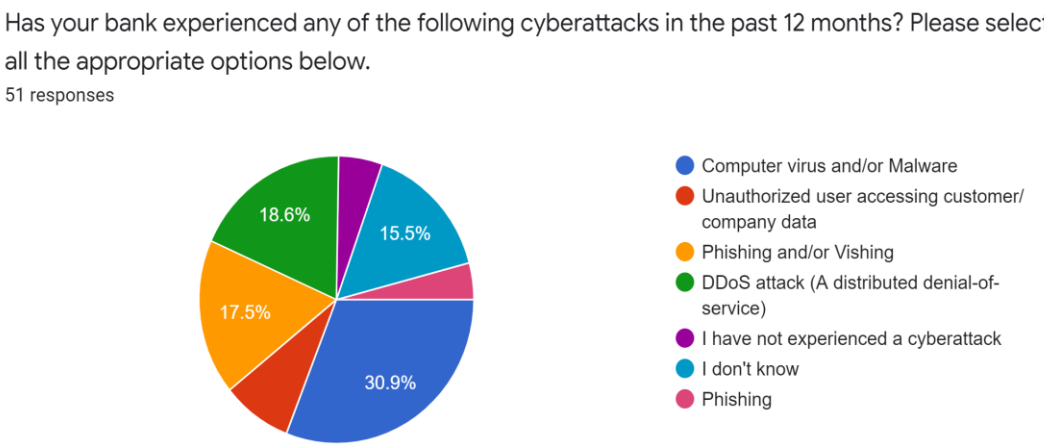


Figure 15: Types of cyberattacks in banks in the past 12 months

This survey question is very important as it identifies the biggest threats in the banking sector. Understanding this provides vital information to the banks as to what specific areas need immediate intervention. In this survey question, 30.9% of the participants selected computer virus or malware attacks as having affected their bank organizations in the past 12 months. Also, 18.6% of the participants stated that DDoS attacks had affected their banks within the same period. Phishing and/or vishing attacks had the third-highest number of respondents, with 17.5% indicating that their banks have been victims in the past 12 months. However, 15.5% said they don’t know if any of the above attacks have impacted their banks in the last 12

months. Also, a small number of the respondents said they had not experienced any attack yet.

The primary benefit of this survey's output is it connects to a previous survey question on the type of antivirus solutions deployed to protect bank systems, where most respondents (60%) indicated that their organizations run an unmanaged and unmonitored antivirus solution. The practice provides a possible explanation as to why banks record higher numbers of computer virus/malware attacks than other attack types. As such, creating awareness on the best malware and virus protection services can enable banks to overcome the attacks. Cybersecurity awareness programs should also touch on other methods for preventing modern attacks.

The presence of phishing and vishing in the top attack vectors shows the need for awareness training for the employees.

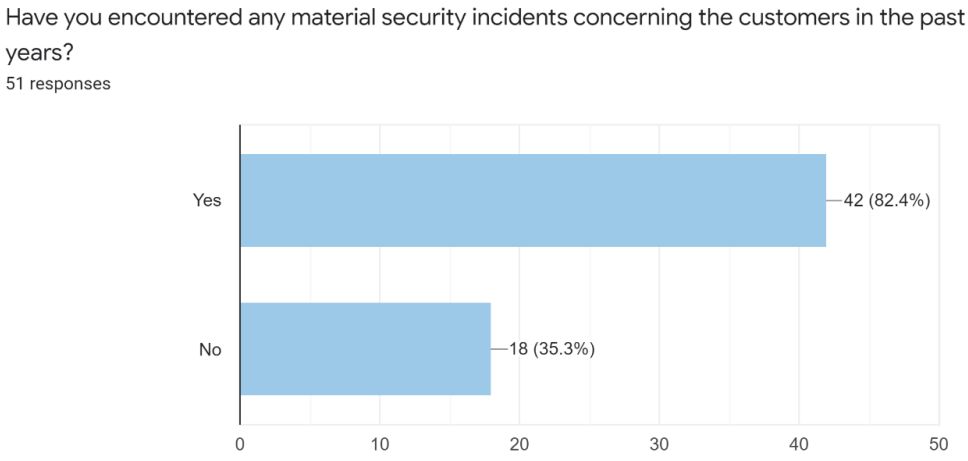


Figure 16: Material security incidents concerning the customers in the past two years

Material security incidents are incidents that have a very high chance on having an operational or financial significance on the customers. This will help us understand the reach of these attacks as far the banks' customers were concerned. A large percentage of the respondents (82.4%) indicated that their customers had been victims of material security incidents in the past two years, while 35.3% said the attacks had not affected them within the same period. This goes to show how widespread the issue of cybersecurity incidents is, with the customers being a very

big victim. The banks can use this information in order to help their customers by providing cybersecurity awareness material, for example through SMS and email. It is essential for the banks in Somalia to create awareness on how their customers can protect themselves from material cybersecurity incidents.

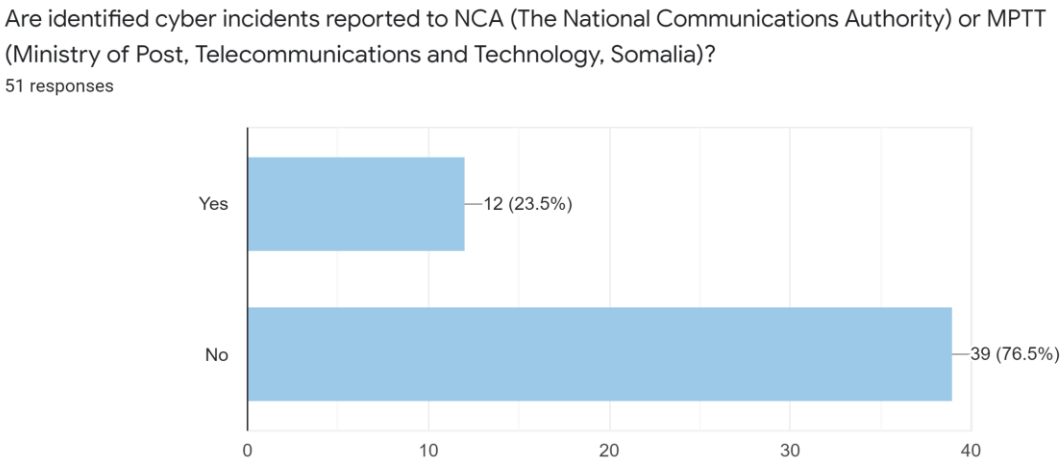


Figure 17: Reporting rate of cyber incidents for banks

Cybersecurity incidents are usually reported to the regulatory bodies as receiving this type of information from banks early and regularly can help the regulators gather intelligence about emerging threats to individual banks and the financial system at large. The NCA is the regulatory body in charge of communication in Somalia but there is no requirement for banks to report any cybersecurity incidents. This survey question is aiming to identify how many banks proactively report the cybersecurity incidents. The survey results indicated that 76.5% of the respondents revealed that their banking institutions don't report identified cybersecurity incidents either to NCA or MPTT.

Somalia does not have a policy or regulation stipulating mandatory reporting procedures of identified cyber threats or incidents, which is why most banks don't report cyber incidents. However, reporting is a recommended cybersecurity practice, and it is, therefore, critical to raise awareness on reporting procedures.

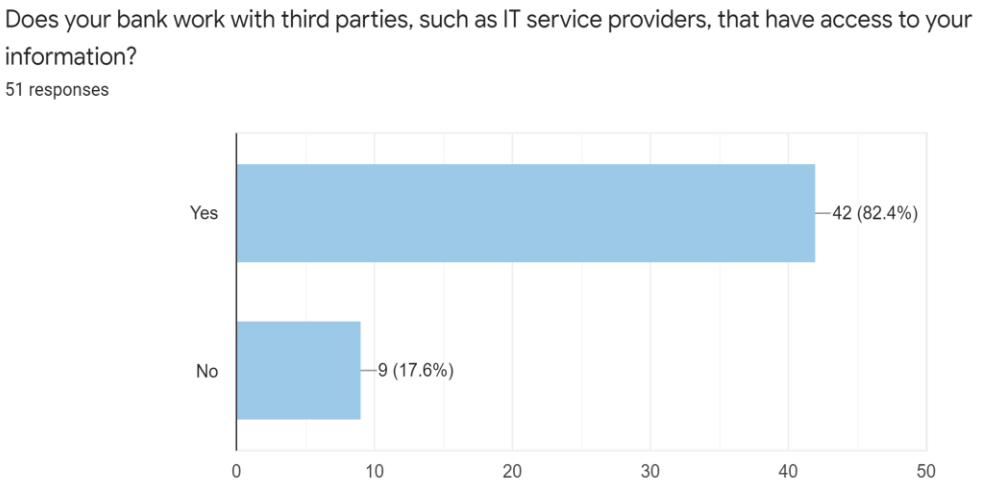


Figure 18: Percentage of third parties with access to bank information

It's no longer sufficient to just guarantee that the organization's systems are protected, there is a need to look into the risk involved in sharing information with third parties. They are external to the banks and thus it is difficult to know what measures are being taken by them to avoid compromise. It is therefore safe to say that third parties increase the attack surface for attackers to access the bank information and infrastructure.

According to the respondents that answered this question, 42 (82.4%) indicated that their bank organizations work with third parties to access their information, while nine respondents (17.6%) said their banks don’t allow it.

The benefit of including this question in the survey is that most banks in Somalia work with external third parties and permit them to access information. It is vital to create awareness of best cybersecurity practices when banks allow third-parties to access sensitive information.

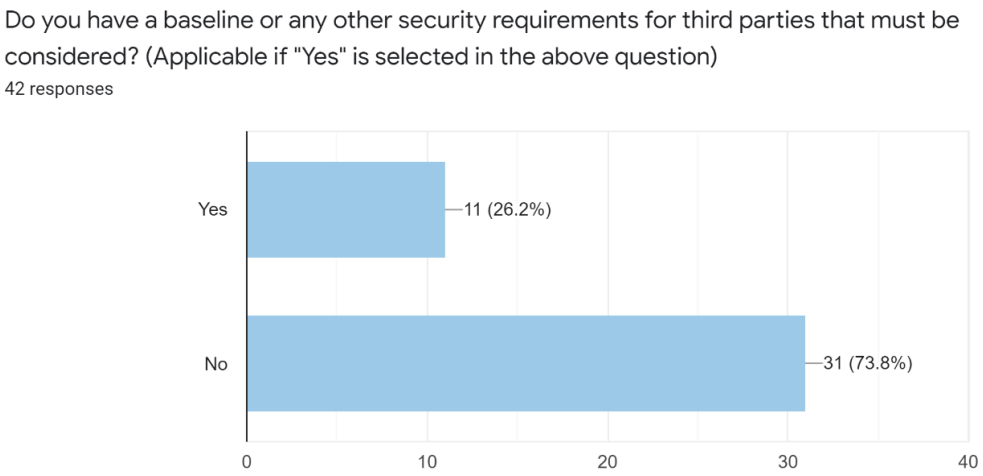


Figure 19: Amount of banks with security requirements for third parties

It is necessary to specify each party's responsibilities when it comes to the requirements needed. This is usually included in the contract with third parties. From the survey's response, 73.8% indicated that their banks don't have any security requirements with the third-parties access to their information. On the other hand, 26.2% of the participants stated that their banks have baseline requirements with their third-parties.

Security requirements with third-parties establish the responsibilities of each party in ensuring data security and privacy. In this case, it is essential to create awareness in the banking sector regarding its importance in data security. It is important to manage third party risk as it exposes banks to supply chain attacks and data breaches.

6.3 Survey on Telecom companies

The survey consisted of 13 questions and involved 20 participants. All survey participants were solely drawn from four telecom companies based in Mogadishu, Hargeisa, Kismayo, and Garowe. The employees involved in the survey hold different positions, and they included supervisors, managers, and C-level executives.

As telecoms are often a gateway into multiple businesses, threats can either target a specific telecom company, its third-party providers, or the subscribers of a telecom

service. This survey looks at how telecoms interact with the above stakeholders, how they protect data within the organisations, and what controls are in place to protect their critical infrastructure. Understanding this would give us the current level of cybersecurity knowledge and awareness within telecom service providers.

The following are the survey results and analysis:

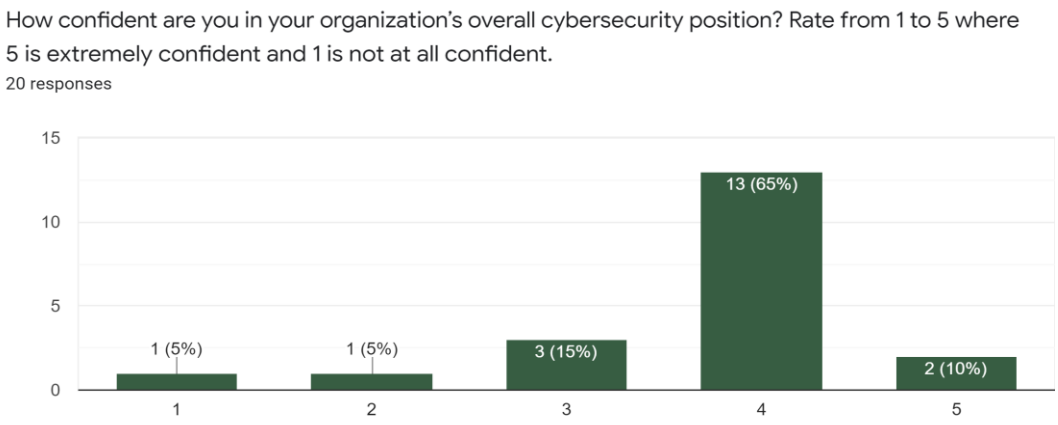


Figure 20: Degree of confidence in the telecoms' overall cyber security position

From the graph, 13 respondents indicated they are confident in their telecom organizations' overall cybersecurity position, and two extremely confident. On the other hand, three individuals indicated they are not sure whether they can trust the cybersecurity posture of their organizations, whereas two individuals were not confident or not at all confident. In general, the results illustrate that at least 65 % of the participants have faith in their telecom organizations implement sufficient cybersecurity processes to safeguard the company's and their personal information.

The output of the survey is encouraging. Firstly, it implies that telecom organizations in Somalia implement some cybersecurity controls, which is why a large number of the respondents are confident with their cybersecurity position. Also, the output is beneficial since it indicates an average cyber awareness level for telecom companies. With a combined total of 75% of respondents having confidence in their company's cybersecurity position, it means they understand the best cybersecurity practices. However, a combined total of 10% are either not confident or not at all confident,

indicating the need to create cybersecurity awareness in the telecom industry and assist telecom providers in Somalia to enhance their cybersecurity posture.

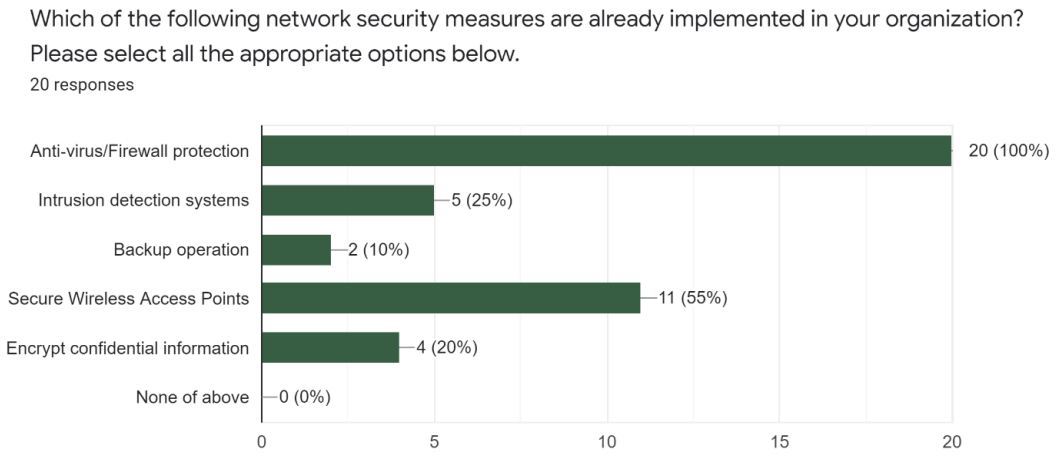


Figure 21: Security measures implemented in the telecom companies

The use of antivirus solutions takes the lion's share as 100% of the respondents indicated that their organizations have already implemented antivirus and firewall protection. However, only 25% of participants agreed that their organizations had implemented intrusion detection systems. Also, 55% of people responding to the survey selected secure wireless access points implemented within their organizations. Although performing a system/info backup operation is recommended, only 10% reported that their organizations perform a system/info backup operation. Encryption of confidential information was not common among the participants with only 20% stating they had this control in place.

Now, the output of this survey question is quite interesting. Antivirus and firewall protection are vital cybersecurity requirements due to malware detection and filtering malicious network traffic. It is no surprise that they are the most used network security measures. However, some organizations are yet to implement the most basic network security measures, which can cause adverse cybersecurity implications. Intrusion detection systems are also vital for preventing network intrusions that may cause data breaches.

What is more concerning is the low number of organizations that perform a backup and implement encryption measures. Encryption is essential to secure customer data by preventing unauthorized access to data at rest, in use, and in motion. Furthermore, regular backups ensure data availability if there is a breach. Failing to implement encryption and system backup measures is a poor cybersecurity practice that can lead to theft of sensitive data.

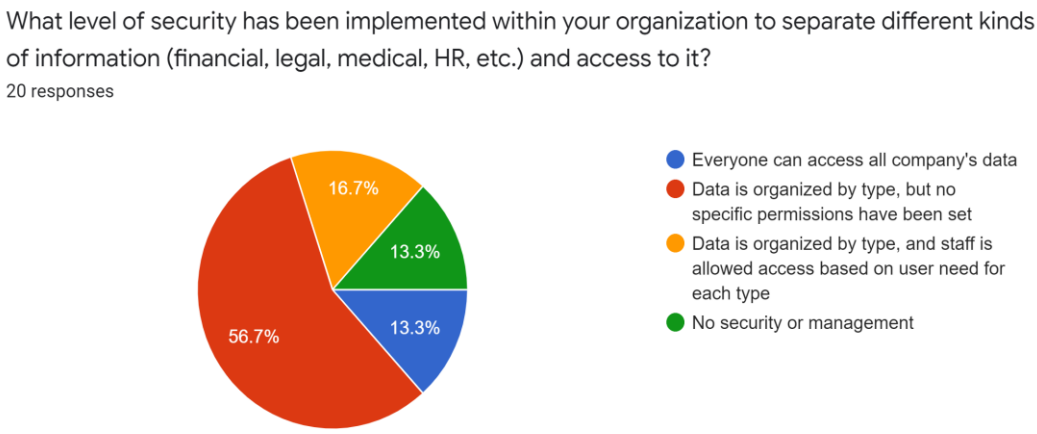


Figure 22: Level of security implementations for data within the telecom companies

This survey question indicated that most telecom organizations in Somalia lack awareness of information security best practices. First, 56.7% of the responses show that telecom companies organize according to types but don't set special permissions. Setting special permissions determines who can access which data and for what reason. However, 16.7% of the responses revealed that their organizations classify data according to type and sets special access permissions, which is a recommended information security practice. Nevertheless, a worrying trend is that 13.3% of the responses show that organizations provide access permissions to everyone despite their roles, while another 13.3% have not implemented policies for managing information security.

A key finding from the survey output is the need to create information security awareness campaigns drawing telecom companies in Somalia. The awareness campaigns should focus on educating telecom providers on the need to implement access control measures, including special access permissions for data already sorted

according to type and depending on employee roles. On a positive note, 16.7% of organizations observe proper information security measures by classifying their data types and setting access control measures for different users. However, the lack of information security awareness can expose telecom organizations to insider threats, data breaches, and unauthorized access or use of sensitive data.

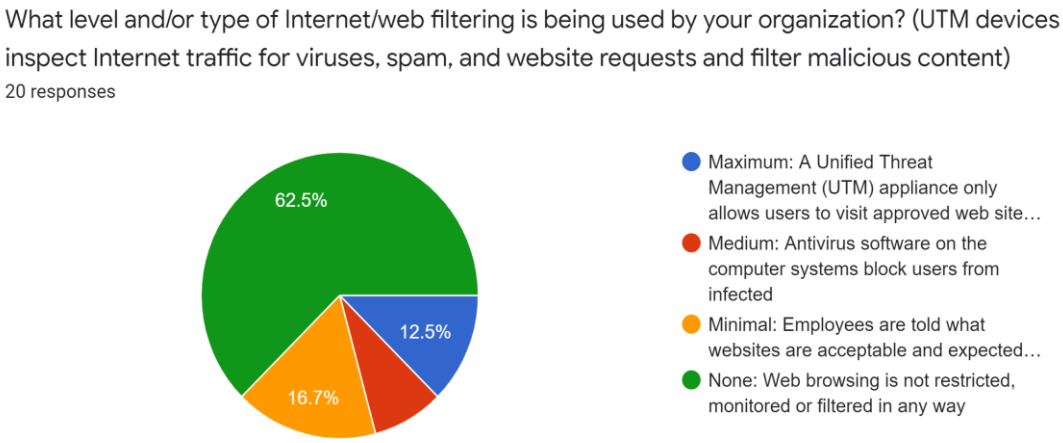


Figure 23: Types of internet/web filtering used in the telecom companies

Internet and web filtering is a critical measure that prevents users from accessing harmful websites that can expose an organization to web-based threats, such as drive-by attacks and malvertising (targeting users with malware-infested ads). Despite the essence of web filtering, a large percentage of 62.5% responses indicate that most telecom companies in Somalia do not restrict web browsing, monitor, or filter web traffic in any way. On the other hand, 16.7 of the responses show that telecom operators only inform their employees which websites are acceptable and which are not but do not implement measures to prevent access to websites deemed harmful. It is, however, encouraging to note that 12.5% of responses reveal that their organizations use a UTM appliance to restrict access to unapproved websites, and less than 10% at least use an antivirus product to block access malware-laden websites.

The key takeaways from the survey output is that telecom organizations in Somalia require awareness on the essence of restricting access to unsafe websites. The awareness campaign should sensitize IT admins on the use of a unified threat

management tool for filtering which websites can be accessed through their organizational networks and computer systems. In addition, employee training is crucial. From the survey results, only 16.7% of responses indicated that their organizations tell them acceptable websites. However, other than creating awareness on the need for UTM, telecom organizations in Somalia should implement training and awareness programs for the employees.

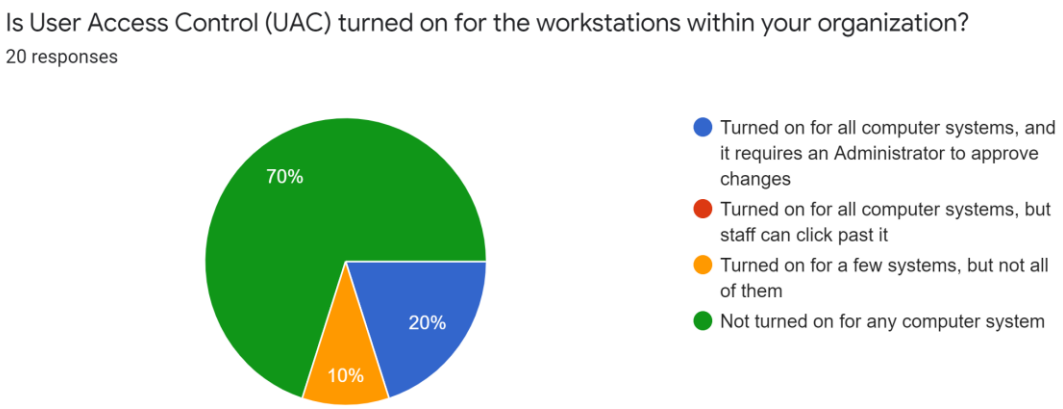


Figure 24: User Access Control utilisation within the telecom companies

Access control systems play a pertinent role in deterring unauthorized access incidents. However, this survey clearly indicates that most Somali-based telecom providers (70%) do not turn on user access control in workstations. An additional 10% of responses reveal that their organizations turn on user access control for some workstations but not all. However, the good news is that 20% of responses indicate that they must request an administration to approve any changes made to a system while access control is turned on for all workstations.

We learn from the survey that there is an urgent need to raise awareness in Somali-based telecom companies of the benefits and importance of enabling user access control in all workstations. Besides, the survey was helpful since it shows that most IT admins are either not aware of the need for turning on access control or lack the skills and knowledge required for the activity. Therefore, all IT admins require a training and awareness program on user access control.

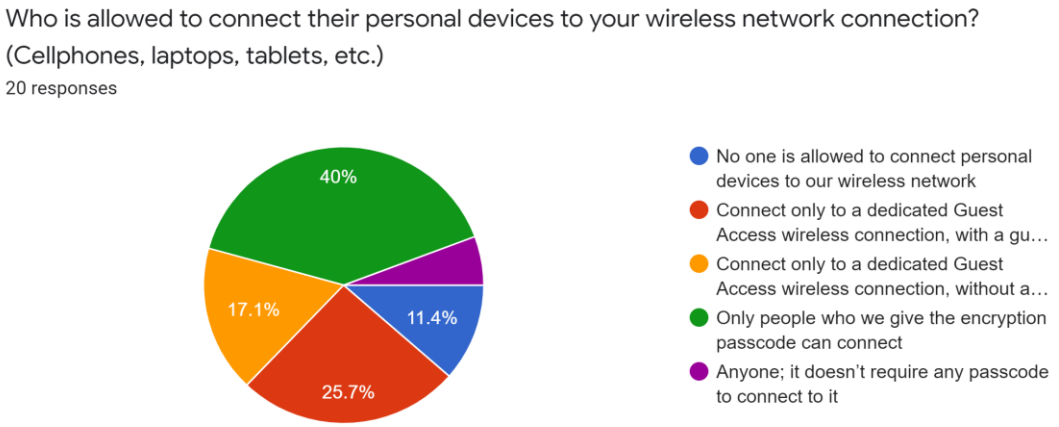


Figure 25: Personal device usage on telecom wireless network connections

The responses to this survey question are diverse. To start with, 40% of the responses indicate that telecom companies allow people to connect their devices to internal networks. This is a risky trend, given that hackers exploit vulnerable personal devices to gain access to a secured network.

Besides, the survey results show that 25.7% of responses agree that their organizations provide a dedicated password-protected guest network for people connecting personal devices. In comparison, 17.1% of responses indicate that the dedicated guest networks are not password-protected. It is, however, encouraging to see that 11.4% of the responses show that their organizations do not allow anyone to connect personal devices to internal networks.

What we see from the survey is that most telecom companies believe that it is safe for anyone to connect to internal networks as long as they obtain the encryption key first. However, this is wrong since any vulnerable device can enable hackers to access internal networks with ease. Awareness programs are necessary to educate telecom providers on the importance of a separate, guest, and password-protected network.

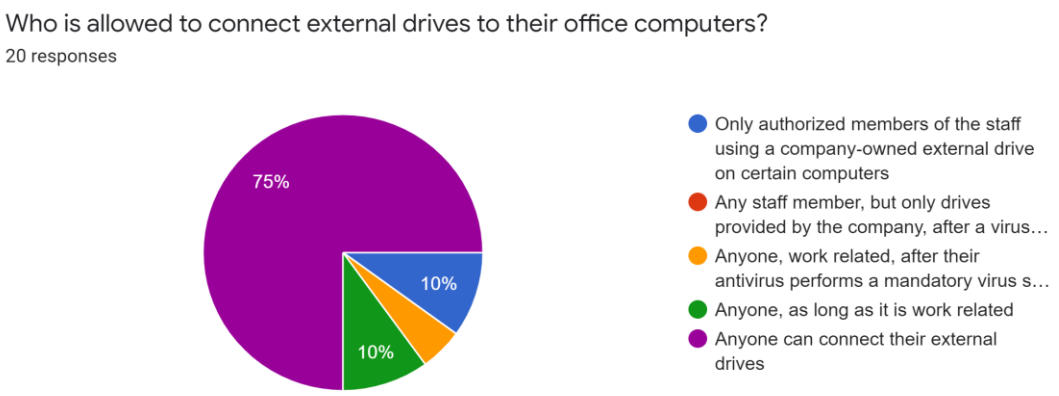


Figure 26: External drivers procedures for office computers in telecom companies

Connecting external drivers to office computers is a risky practice since malicious individuals can load harmful programs and introduce them to a secured environment. As indicated in the pie chart above, 75% of responses indicate that companies allow anyone to connect external drivers to office computers. It was also interesting that 10% (the green pie) of responses showed that anyone could connect external drives to office computers as long as it is work-related. Moreover, it was impressive noting that 5% indicated that anyone could connect a work-related external drive but after running a mandatory antivirus scan. However, only 10% (the blue pie) recorded the recommended standard since their organizations only allowed authorized staff members to connect company-issued external drives on specific computers.

The main concern from the survey's output is that a massive 75% of the participants indicated that anyone could connect an external drive. That policy exposes the organizations to multiple cybersecurity threats, including insider threats working in cahoots with cybercriminals to infect specific computers using infected drivers and unauthorized copying of sensitive information. In this case, a cyber-awareness campaign on the use of external drives should be done in earnest until all organizations observe policies similar to those of the blue pie chart.

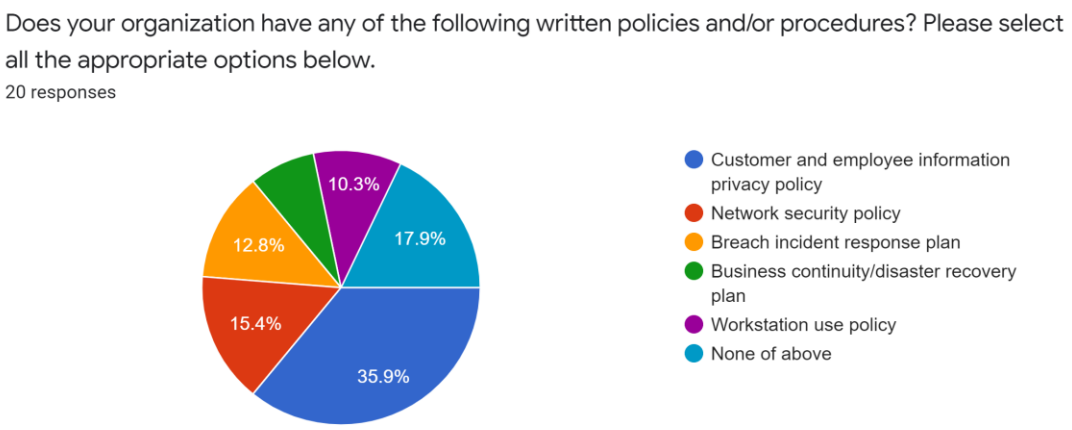


Figure 27: Available information security programs for monitoring systems in telecom companies

From the above pie chart, organizations with customer and employee information privacy policies hold the largest share of 35.9%. Moreover, 15.4% response shows organizations that have a written network security policy. It is also worth noting that 12.8% of the responses show the organizations with a written breach incident response plan. In comparison, less than 10% have a written business continuity and disaster recovery policy. However, a small 10.3% have a workstation use policy despite being one of the most vital written cybersecurity procedures. Nevertheless, the most worrying result from the survey is that 17.9% of the responses indicate organizations without a written cybersecurity procedure.

The advantage of conducting this survey is that 17.9% of the total respondents revealed that their organizations lack a written cybersecurity procedure. Also, the survey's output showed that telecom companies are most aware of customer and employee information privacy policy and least aware of business continuity and disaster recovery policies. Therefore, any cybersecurity awareness campaigns in the region should concentrate on raising more awareness on the application of business continuity and disaster recovery plans, and also educate how to maintain robust, written cybersecurity policies.

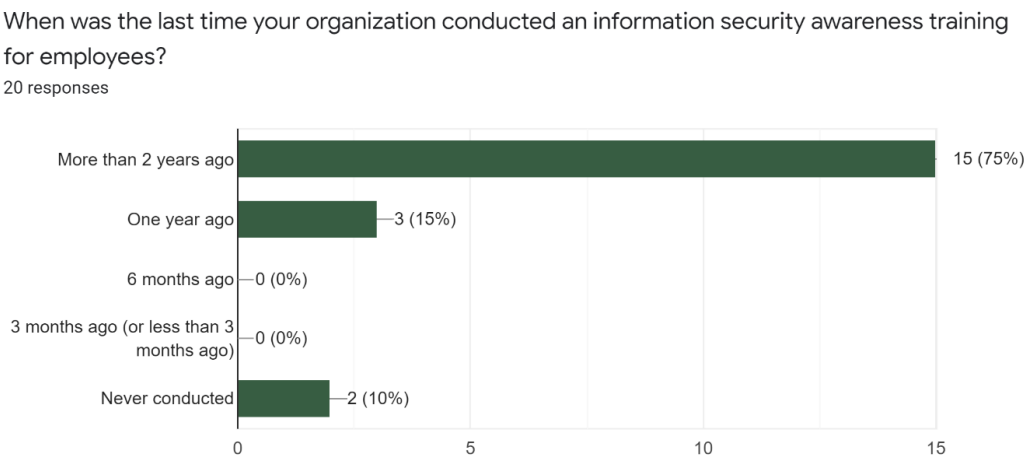


Figure 28: Regularity of employee information security awareness training in telecom companies

Conducting frequent information security awareness training programs enlightens employees on how to identify and manage modern cybersecurity threats. The recommended frequency for refresher training courses is quarterly (every three months). From the bar graph above, 75% of the respondents indicated that their organizations conducted training awareness programs more than two years ago with 15% having one more than one year ago, respectively. It is, however, concerning that two participants (10%) revealed that their organizations have never conducted an information security training and awareness program.

The survey's result was beneficial since we were able to identify that all of the telecom organizations in Somalia need to implement immediate training programs for their employees. Failure to do so may continue exposing them to numerous cyber threats since humans are the most vulnerable in organizational cybersecurity. Examples of possible attacks due to untrained employees include phishing, whaling, and targeted identity theft.

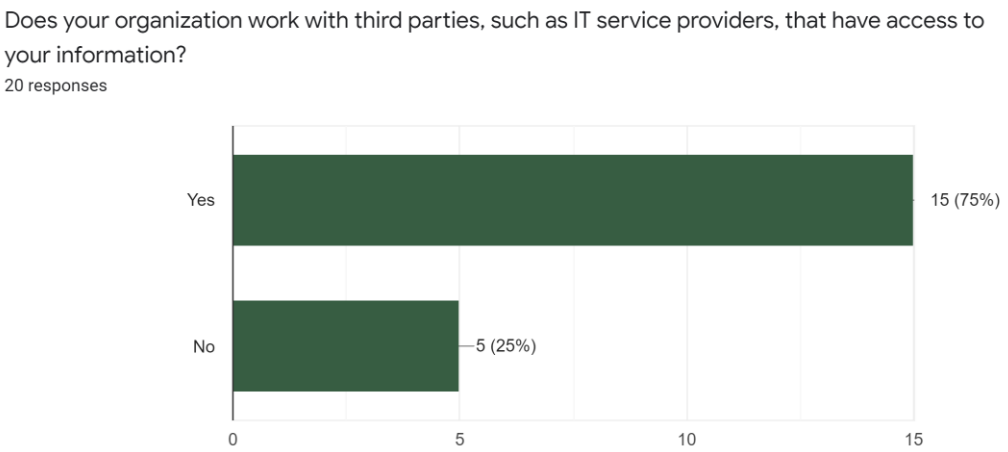


Figure 29: Percentage of third parties with access to telecom information

Third parties, such as IT service providers, are critical to organizations operating in the telecom industry. From the above data, 15 respondents (75%) agreed that their organizations provide information access to third-party IT providers, while five respondents (25%) said no.

The advantage of including this question in the survey is it helped us understand that majority of telecom companies work with third parties. Therefore, it is pertinent to create awareness of how they can protect themselves from third-party cybersecurity risks. For example, an awareness campaign sensitizing telecom organizations to conduct a risk assessment on all third parties is essential.

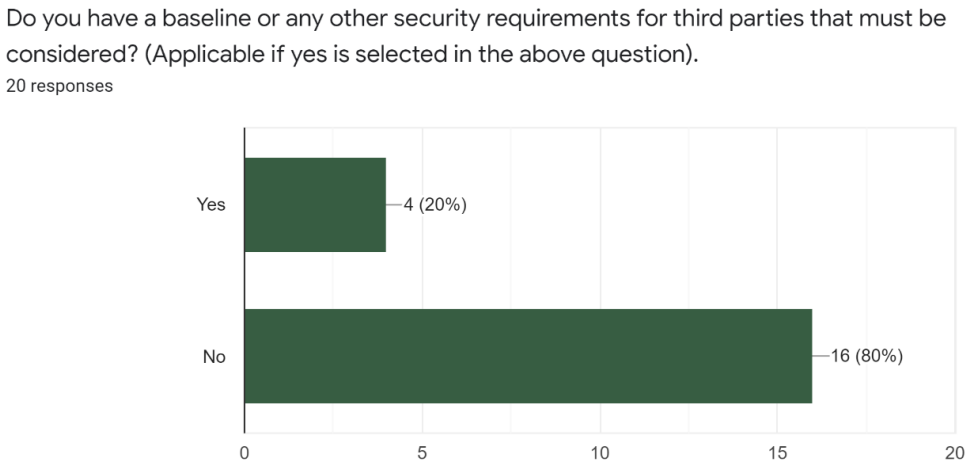


Figure 30: Amount of telecom companies with security requirements for third parties

A Business Agreement (BA) or contract is a written procedure that specifies all parties' responsibilities. Most contracts do not include security requirements in areas dealing with handling of sensitive information. From the survey's results, only 20% of the respondents are sure that their telecom organizations have a business agreement, while 80% do not.

The survey's output reveals that most telecom companies lack any security requirements for third parties. Telecom companies hold a lot of private data on customers and employees. This creates a problem as the country does not have strict data protection regulations so there is no regulator on the third parties. Despite that, BA assists organizations in strengthening privacy and security measures implemented to protect confidential information. That said, a cybersecurity awareness should be done in Somalia to sensitize telecom organizations on how to add security requirements in contracts with third parties.

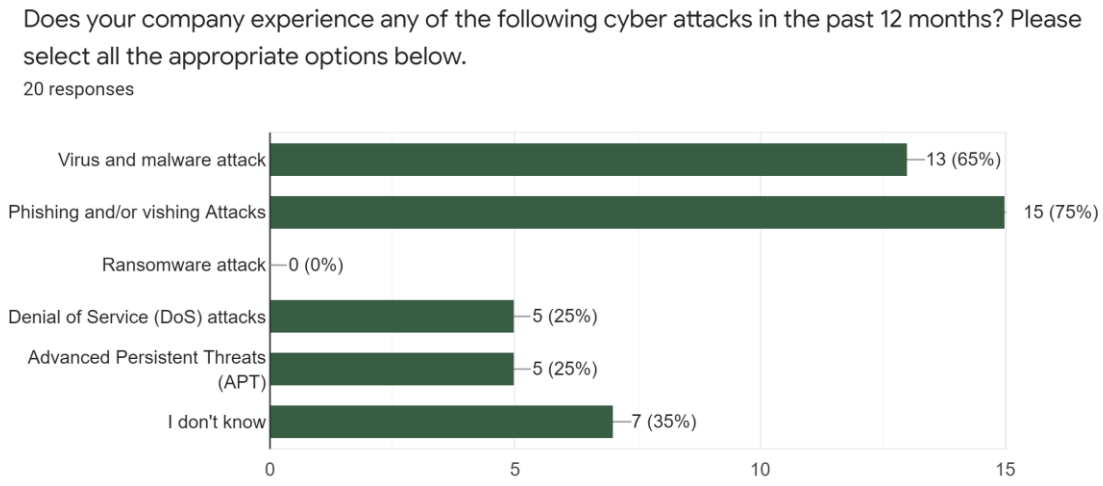


Figure 31: Types of cyberattacks in telecom companies in the past 12 months

Phishing and/or vishing attacks dominated the types of cyber-attacks that targeted telecom organizations in Somalia in the past six months, accounting for 75%. Also, 13 people (65%) said that virus and malware attacks affected them within the same period. On the other hand, DDoS attacks and advanced persistent threats had the lowest percentage, each recording 5% of affected organizations. Seven of the participants were unsure whether any of the attacks had affected their organizations.

The primary benefit of this survey's output is it connects to the survey question on information security awareness training, where most respondents indicated that their organizations last conducted a training campaign more than two years ago. Numerous researchers agree that poorly trained users are more susceptible to phishing and other social engineering attacks. In this case, telecom organizations in Somalia need to expose their employees to more cybersecurity training and awareness programs. Furthermore, it is vital for organisations in the region to understand the best strategies for protecting themselves from malware attacks.

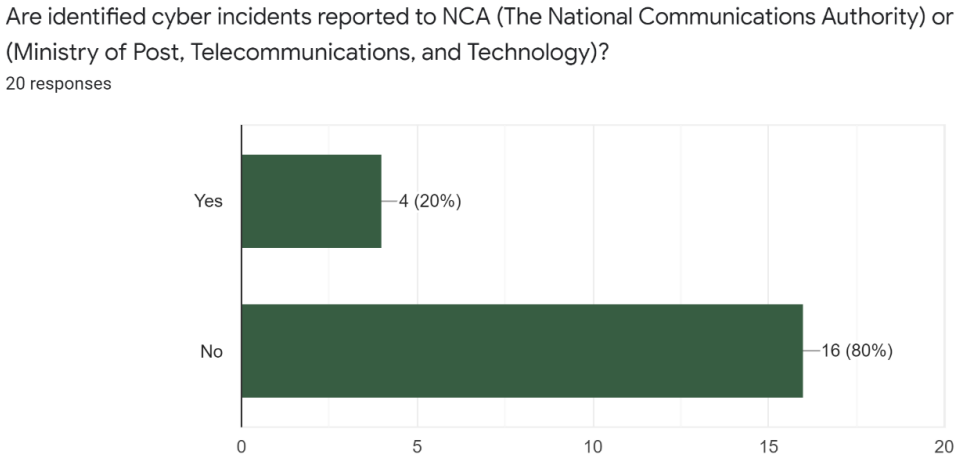


Figure 32: Reporting rate of cyber incidents for telecom companies

The National Communications Authority is the regulatory body in charge of communication in Somalia. It is required that all incidents are reported to the NCA through the Somalia CERT. From the bar chart above, it is clear that 80% of organizations included in the survey do not report cyber incidents, while only 20% do. It is essential to raise awareness there and should be a policy requiring affected organizations to report cyber incidents to the NCA and MPTT.

6.4 Survey on Government Institutions (NCA & MPTT).

This survey targeted participants drawn from the National Communication Authority (NCA), the Ministry of Posts, Telecom, and Technology (MPTT). These institutions are responsible for the country's cybersecurity, with the former (the NCA) having more

responsibilities. The participants comprised staff members, employees, and managers.

The questions in this survey aimed to understand:

- barriers to cybersecurity development within Somalia.
- the cybersecurity policies and strategies set up.
- the capability to counteract breaches, incidents and attacks.
- the actions taken to improve cybersecurity in the country.

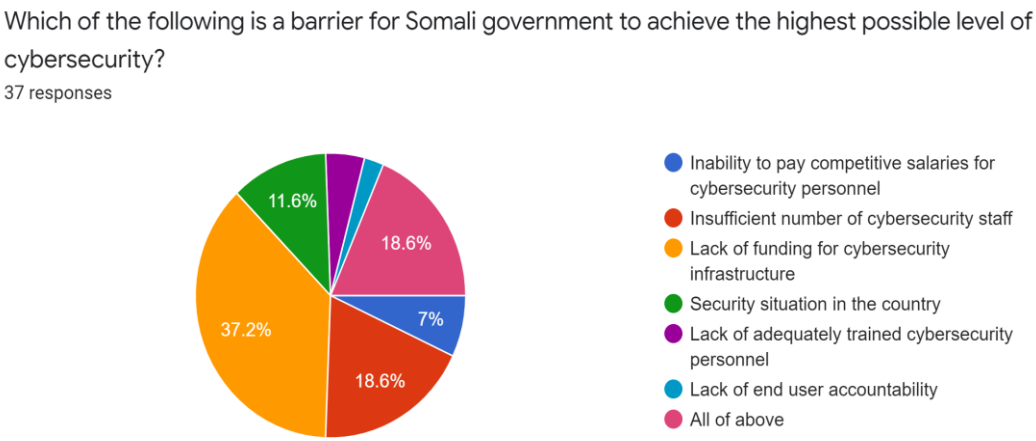


Figure 33: Barriers for Somali government to achieve the highest possible level of cybersecurity

Understanding what prevents Somalia from achieving its cybersecurity goals is crucial as it affects what activities can be undertaken. Identifying these issues is important as it helps us address the causes and effects and work towards removing them. The Somali government's primary barrier to achieving optimum security is inadequate funding for cybersecurity infrastructure, with 37.2% of the participants stating so. Also, 18.6% said that an insufficient number of cybersecurity staff is also a challenge for the government. Another 18.6% indicated that all of the listed issues were barriers to achieving maximum cybersecurity protection. On the other hand, 11.6% attributed the inability to realize the highest possible cybersecurity level to the country's security condition. A further 7% attribute the challenge to inability to pay competitive salaries for hiring and retaining cybersecurity experts.

The benefit of conducting this survey is that it sheds light on the main barriers preventing the Somali government from achieving adequate cybersecurity. Inadequate funding is indeed a challenge since it prevents the government from investing in modern cybersecurity procedures.

Furthermore, the survey revealed that Somalia is facing an acute shortage of skilled cybersecurity personnel, which is a global issue. Most of the barriers point towards financial constraints. Therefore, it is necessary to raise awareness on the essence of investing heavily in cybersecurity equipment and personnel to achieve the desired security level.

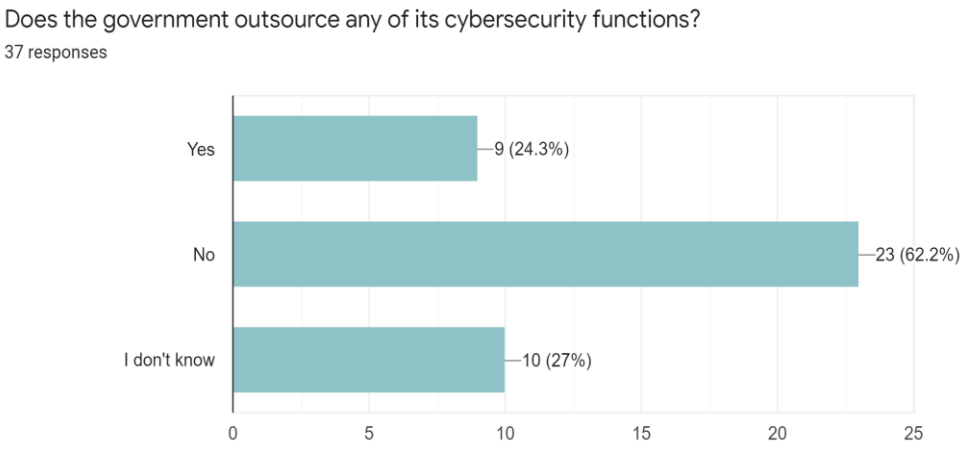


Figure 34: Percentage of government outsourcing cybersecurity functions

From the survey, 62.2% of the participants indicate that the government does not outsource cybersecurity functions, while 24.3% believe it does. However, 27% are unsure if the government outsources any of its functions.

Outsourcing cybersecurity functions has proven to be an effective method of achieving high cybersecurity levels but at reduced costs. With the first survey question showing that financial constraints are the primary reason why the government cannot achieve the highest possible cybersecurity levels, it goes to reason that the government would not outsource critical cybersecurity functions. The government therefore attempts to do a lot of the work itself in an attempt to lower costs, despite the fact that outsourcing can actually reduce costs as there is

zero investment on security infrastructure. It is, therefore, necessary to create awareness on why the government should outsource most of its cybersecurity processes.

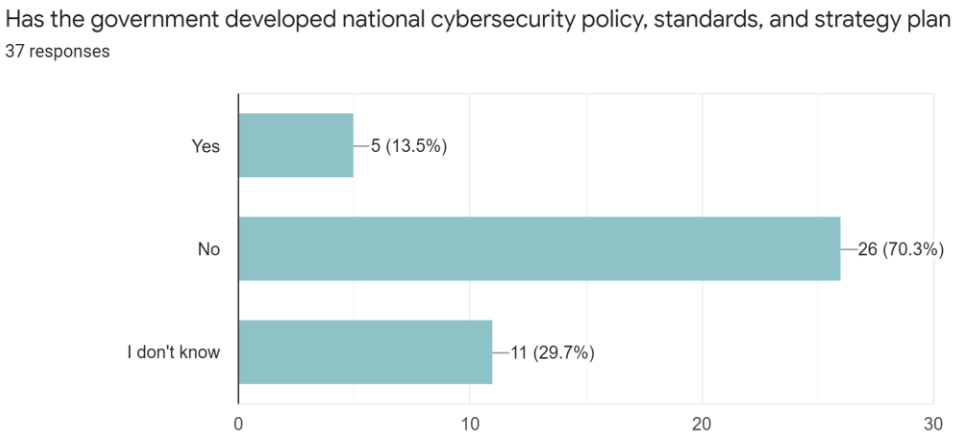


Figure 35: Rate of development of national cybersecurity policy, standards, and strategy plan

The responses to this survey question show that the Somali government has not developed national cybersecurity policies, standards, and strategy plans as indicated by the 26 respondents, or 70.3%. However, 13.5% believe the government has developed compliance regulations. It is of utmost importance to raise awareness on why the government should develop strong policies and standards immediately. They are crucial to enabling all entities processing personal data within the country to achieve the same cybersecurity posture.

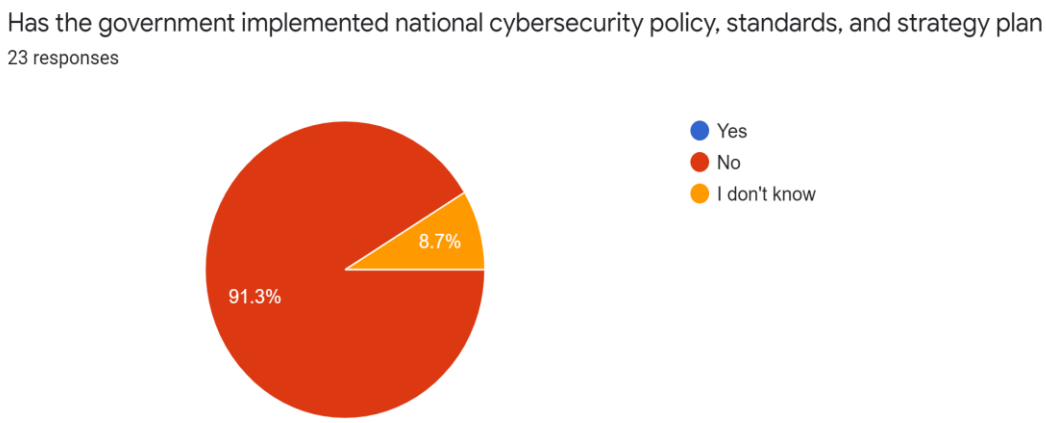


Figure 36: Implementation rate of national cybersecurity policy, standards, and strategy plan

A resounding response of 91.3% shows that the Somali government has yet to implement national cybersecurity policies, standards, and strategy plans. Although the responses were only 23, it indicates that other nations are leaving Somalia behind since it lacks National cybersecurity guidelines stipulating the minimum cybersecurity standards all organizations must adopt to maintain robust cybersecurity processes.

Therefore, the relevant agencies must legislate the necessary compliance standards and requirements that protect data at the national and international levels. The relevant authorities require to adopt compliance standards and regulations that provide the same cybersecurity level, such as the EU General Data Protection Regulation (GDPR). The National ICT policy and strategy (2019-2024) mentions an establishment of cybersecurity strategy, it is yet to be commenced.

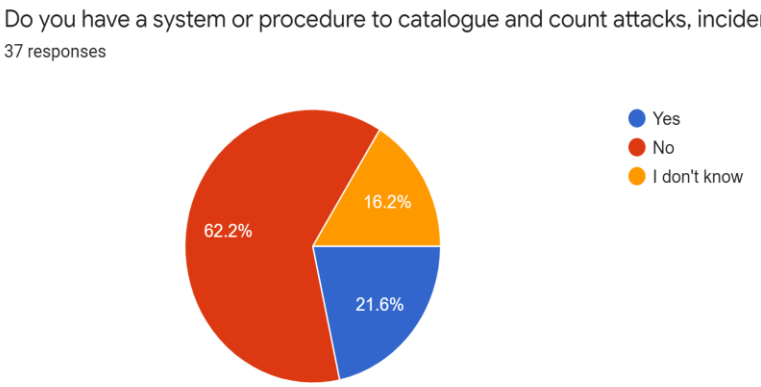


Figure 37: Presence of systems or procedures to catalogue and counter attacks, incidents, and breaches

Having the capacity to catalogue and count adversarial incidents is necessary to manage national cybersecurity since the government can evaluate if the deployed countermeasures are working. However, 62.2% believe that the government does not have a system for counting breaches, while 21.6% said the government has the capabilities. A partial 16% was unsure.

The survey output shows that the Somali government needs to invest in the right procedures or systems for tracking attacks and incidents to monitor its ability to reduce the cyber risks facing the country. The Somalia CERT should commence the process of identifying and recording cybersecurity incidents and breaches.

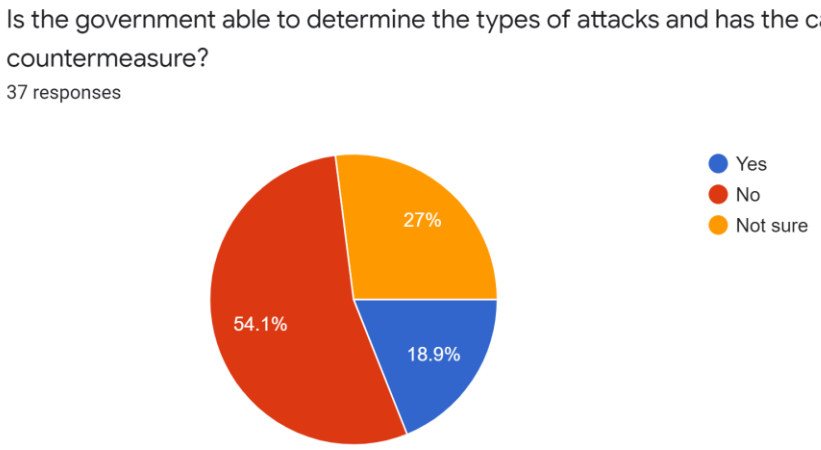


Figure 38: Capability of government to determine the types of attacks and the capacity to countermeasure

Being able to determine the types of attacks is the first step to preventing them. Once these attacks have been recognized, the government should then be able to provide countermeasures to them. According to the survey results, 54.1% of the participants lack the ability to determine the types of attacks or the capacity to mitigate them. However, only 18.9% are sure the government has the capacity to identify and deal with various types of attacks, while 27% are unsure. In this case, it is critical for the government to invest in the lacked cybersecurity tool, personnel, and procedures to immediately identify the type of attack and implement countermeasures.

The ability to identify and countermeasure attacks is critical to a country. Majority of the attacks can spread to several machines in a span of time, if not halted. For example, if a government entity has been infected with the NotPetya virus, the ability to identify it is crucial as there is a technique available to prevent it from executing.

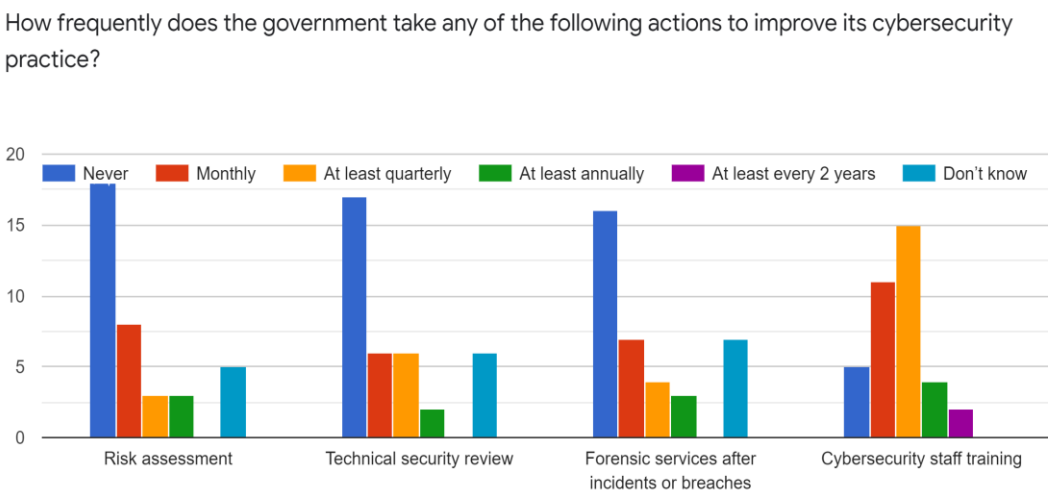


Figure 39: Frequency of the government to take actions that improve its cybersecurity practice

From the above bar chart, the blue stands out for risk assessment, technical service review, and forensics services after incidents or breaches, which is for never. On the same charts, the respondents stated that the government conducted monthly activities, with the red bar being the second most dominant. Furthermore, a few participants indicated that the government performs the actions at least quarterly and annually. However, the bar chart on cybersecurity awareness training shows a high frequency where 15 participants said that the government conducts awareness training at least quarterly.

What we can learn from the survey output is that the government places little emphasis on risk assessment, technical security review, and forensics services after incidents or breaches. However, these are critical aspects of maintaining robust security, and it means that the responsible governmental agencies may not be aware of the benefits of performing the aforementioned actions frequently. Although the government prioritizes cybersecurity awareness training in its measures to improve cybersecurity, it is still insufficient.

7 Research Discussions

A high-level discussion covering the previous chapters provides deeper insight into the outcomes disclosed during the research. The research's primary aim was to evaluate the current cybersecurity state in Somalia, the main cybersecurity challenges in the public and private sectors, and what organizations in both sectors are doing to address them.

7.1 The objectives

In this case, the main objectives driving the research was:

- Identify cybercrimes and threats.
- Analyse the current cybersecurity awareness in Somalia.
- Recognize best practices from several successful countries as well as from less developed countries.
- Provide recommendations on cybersecurity areas to be selected in future awareness campaigns.

A mixed approach research methodology was used to analyse the level of cybersecurity awareness in the country. A qualitative method was used to identify and analyse cyber threats and their impact. We also analysed cybersecurity activities from different countries to discover what they are doing to combat cyber threats. A quantitative methodology was used to gather relevant data from different stakeholders by use of a questionnaire. The study involved the private and public sectors and it, therefore, used four different surveys targeting different sectors. They are public awareness, telecom companies, banks, and government institutions. The results of the entire survey are as discussed in the following sections.

7.2 The results

The surveys targeted various individuals working in different sectors to gather relevant data regarding the cybersecurity awareness level in Somalia. Hence, the surveys comprised different questions, and the results were equally varied. However, the results were a clear indication of the current cybersecurity state in Somalia,

cybersecurity awareness level, as well as the level in which institutions in the private and public sectors have implemented cybersecurity strategies and policies.

The information collected in the surveys can be used by organisations within the different sectors to implement a cybersecurity awareness. The following are detailed discussions of the surveys' results:

Public Awareness Survey

The survey targeted random members of the public not associated with any organization. Most participants indicated that they use the internet for online banking/money transfer, while studying and research recorded the second most reason. Activities like running a business and using the internet for email and social media had lower responses. However, one of the identified risks in Somalia currently is a remittance-based economy, where Somalis utilize enterprising firms to send and receive capital. With numerous mobile payment firms coming up and the majority of the public using online mobile payment services at least two times a week, it is pertinent to raise awareness on best cybersecurity practices. Besides, financial cybercrimes are common in Somalia as both young local hackers and international cybercriminals commit them.

In addition, the majority of individuals in Somalia learn about cybersecurity from the workplace. From the survey results, a majority of individuals are also self-taught whereas a quarter of them lack any cybersecurity knowledge or awareness. The result echoes a previous finding on cybersecurity awareness in Somalia that showed the core challenge for the Somali government is a dire lack of public cybersecurity awareness, in addition to a lack of national cybersecurity awareness campaigns**.** Adversaries target human weaknesses since they are easy to execute with simple social engineering attacks. Addressing the challenge is essential to enabling Somalia to achieve a more robust cybersecurity posture.

Also, the survey evaluated the kind of security measures the public has implemented personally by listing four measures in the survey question. However, almost a third indicated that they have not taken any of the measures for personal protection. The results reflect a concern noted earlier of the inability of Somalia's internet users to

protect themselves adequately from cyber-attacks. The internet penetration rate is still expanding; thus, most internet users are a novice and not technically competent (Kshetri, 2019)**.** That said, a cyber-unaware population lacking the skills to defend themselves from attacks means the current state of cybersecurity in Somalia is wanting.

Another notable trend in Somalia's cyber threat landscape is more than half of the population has encountered scams done through phones, emails, and online games. According to the participants involved in the survey, the majority stated that they have encountered the attacks. The problem of social engineering attacks is not unique to Somalia as it is prevalent in other parts worldwide. Phishing attacks are popular since they provide attackers with an easy of compromising confidential information for malicious use (Rapid7, 2020).

Survey on Bank Institutions

The survey targeted participants working in the banking sector, including managers, staff members, and employees, drawn from the top four banks. A high percentage of the survey participants indicated that they are not sure whether they are confident with their bank’s cybersecurity position or not, which is a significant number. A smaller percentage indicated that they are not confident. This large number may be due to a lack of robust cybersecurity and data protection policies that govern sensitive information.

Besides, Bashir (2019) argues that the lack of formal regulatory banking structures and sophisticated relationships between the legal systems complicates the ability of the government to resolve and regulate money conflicts, such as inaccurate transactions, scams, and disputes over transfer volume. Such challenges explain why most people in the banking sector may be unwilling to trust their banks’ cybersecurity posture.

In addition, the survey shows that most banks in Somalia rely on antivirus or firewall protection as almost all of the participants indicated their banks have already implemented as a network security measure. Nevertheless, most of the banks with antivirus deployments run paid-for standalone antivirus products that are

unmonitored or unmanaged, which are inadequate to protect against modern cyber threats. Also, half of the respondents indicated that their bank institutions have implemented intrusion detection systems.

However, fundamental network security measures, such as system/info backup operations, username-password management, and encrypting confidential information stored on portable devices had lower responses. Failing to invest in basic but essential cybersecurity measures shows laxity in Somalia's banking institutions to protect themselves from adversarial events. The implication makes sense as Kshetri (2013) implies that most African countries perceive cybersecurity as a luxury rather than a requirement as cybersecurity budgets are estimated to be less than 1% of the total budget. As such, it is accurate to say that banks in Somalia are yet to accept or appreciate the significance of robust cybersecurity measures.

The survey also revealed a lack of information security awareness among banks in Somalia. For instance, half of the respondents stated that their bank organizations organize data according to type but do not set specific access permissions for different users. Furthermore, a small percentage stated that their banks allow all employees to access sensitive information despite their roles, whereas some indicated that their banks lack an information security management policy.

A similar trend was noted in a different survey question, where half of the participants indicated that their banks allow any staff member to connect external drivers to their office computers, and a quarter allow anyone to connect including visitors. Such practices are risky and threaten the confidentiality, availability, and integrity of sensitive customer or employee information. On the same note, a separate question revealed that half of the banks in Somalia last conducted an information security awareness training program more than two years ago, whereas 12.9% have never performed any security assessment.

The results are a clear indication that most banks don’t adhere to best information security practices. Anderson (2001) and Chubb (2019) provides primary steps for securing employee data and recommended information security measures, respectively. They include developing formal, written information security policies,

educating employees on best information security practices, restricting access to employee roles, and implementing data protection policies.

It is also worth noting that a third of the respondents said that their banks have experienced computer virus and/or malware attacks in the past 12 months. DDoS attacks were also common attacks targeting bank accounts in Somalia with 15.5% of the participants stating that their banks have encountered them in the past 12 months. The result shows that malware attacks are more prevalent compared to others, which may be because of dependence on unmonitored and unmanaged antivirus deployments.

Moreover, according to Symantec (2016), cyberattacks affecting Somalia's institutions is due to a lack of proper cybersecurity standards. For example, pirated software is inexpensive and common among users, but it cannot be upgraded with security patches or updates, therefore spreading malware rapidly. It is vital to create awareness on preventing malware attacks and the essence of using monitored, managed solutions to detect malware in real-time.

Lastly, a majority of the survey participants stated that their bank institutions don’t report cybersecurity incidents to NCA or MPPT. Reporting incidents is a recommended cybersecurity practice since it enables the relevant authorities to investigate and evaluate the national cyber preparedness, and also informs what to prioritize to maintain a robust national security posture. However, the main challenge facing the Somali government is the need to implement national strategies and regulations for controlling and monitoring cyber incidents in the country.

Survey on Telecom Companies

The survey used to survey cybersecurity state and awareness in the telecom sector contained 13 questions and involved participants drawn from four telecom companies. The participants included supervisors, managers, and C-level executives. Some of the results are similar to those of the bank survey since some of the questions were used in both surveys.

To begin with, most of the participants indicated their confidence in the cybersecurity position of their organizations. According to Stremlau (2012) flawed law enforcement and rules are a cybersecurity concern but have not stopped telecom companies from expanding and thriving despite the lack of a state regulatory culture.

Additionally, all of the participants stated that their organizations rely on antivirus and firewall as the primary network security measures, whereas only a quarter indicated using intrusion detection systems. The results are similar to those revealed in the bank survey where antivirus/firewall security has the most responses followed by intrusion detection systems. Similarly, fundamental network security measures, including information backup operations and encryption, are not common requirements among Somali telecom companies.

Also, information security awareness in Somalia's telecom industry is wanting. Half of individuals responding to a survey question indicated that their organizations organize the data according to type but do not set specific access permissions, whereas 13.3% indicated that anyone can access all data despite their roles.

In a separate survey question, most of the participants indicated that their organizations have not turned-on user access control for any computer system, meaning anyone can access information stored in those computers/systems. Besides, many others indicated in a different survey question that their organizations allow anyone to connect external drivers to office computers. A further 65% stated that their companies have not exposed employees or contractors to information security awareness and training for more than two years. Therefore, companies in the telecom industry require to develop information security policies governing the access of specific types of data. The policies should be based on the information security practices recommended by Anderson (2001) and Chubb (2019).

The survey also evaluated internet filtering strategies in telecom organizations and the results indicated a lax in cybersecurity protection. According to 62.5% of the participants, their organizations do not restrict, filer, or monitor web browsing while only 16.7% stated that their companies tell staff members acceptable websites but

do not create or enforce policies on the same. Web monitoring and filtering is a proactive cybersecurity measure for identifying and preventing attacks before they can compromise sensitive data and systems. Besides, Richard A. Clarke (2019) postulates that cybersecurity parameters should not only be limited to robust network security but should also align with associated components, filtering, and intrusion detection and prevention systems.

Furthermore, 40% of respondents stated that their organizations provide encrypted password codes for anyone asking to connect to their wireless network connections. However, permitting all and sundry to connect personal devices places a network at risk of malware or DDoS attacks. As stated earlier, many internet users in Somalia lack cyber awareness on the best practices to protect their personal devices. Allowing any user to connect to a wireless network might result in insecure connections providing a point of entry for hackers. It is pertinent for the telecom industry to implement appropriate network access policies to counter network attacks.

The survey's results also show that phishing and/or vishing attacks are more common in the telecom industry, with 75% of the participants indicating that the attacks have affected their organizations in the past 12 months. Also, 65% of the participants indicated that their organizations have been victims of virus and malware attacks.

The prevalence of both attacks can be attributed to the telecom companies relying on traditional security solutions to protect against modern malware threats whereas the lack of web browsing filtering or monitoring permits users to access phishing websites hence exposing their organizations to phishing and vishing attacks. It is vital for telecom companies to invest in managed and monitored security systems to protect against malware and virus attacks and deploy sufficient web monitoring systems to monitor user activities and detect attempted phishing attacks.

Lastly, 80% of the participants indicated that their organizations don't report cyber incidents to NCA or MPTT. It is the same trend observed in banks but attributed to an unregulated ICT environment in Somalia.

Government Survey

A survey evaluating the state of cybersecurity and awareness in the Somalia government agencies involved participants drawn from NCA (National Communications Authority) and MPTT (Ministry of Information Technology and Communication).

The most notable result from the survey is 37.2% of the participants blamed the lack of funding for cybersecurity infrastructure as the leading cause of why the Somali government is unable to achieve the highest possible level of cybersecurity. An additional 18.6% indicated that an insufficient number of cybersecurity staff also prevents the government from achieving robust cybersecurity processes, while 11.6% attribute the challenges to the security situation in the country.

According to Gagliardone & Sambuli (2015), it is difficult to enforce rules and regulations in Al-Shabaab-controlled regions. Inadequate funding is a common challenge in most African countries, but it is more prevalent in Somalia due to the lack of ICT infrastructure and the security problem in the country. Also, 62.2% of the individuals participating in the survey indicated that the government does not outsource any cybersecurity functions. Outsourcing cybersecurity can enable the government to achieve the desired cybersecurity level since managed security providers (MSPs) use the latest cybersecurity procedures, tools, and professionals to provide cybersecurity functions at minimal costs.

Furthermore, 70.3% of the respondents indicated that the government is yet to develop national cybersecurity policies, standards, or strategy plans. Failing to develop national cybersecurity standards has a significant impact on national cybersecurity due to the lack of formal guidelines for deploying cybersecurity protection systems, securing critical infrastructure, and preserving information integrity, confidentiality, and availability.

An additional 91.3% indicated that the government has not implemented national cybersecurity policies, which makes sense since the government is yet to develop them in the first place. Besides, 62.2% of the participants stated that the government lacks procedures for cataloguing and count cyber incidents and breaches. Also, 54.1%

stated in a different survey question that the government is unable to determine the types of attacks and lacks the capacity to implement required countermeasures. The inadequacy shows that Somalia lags most nations in its cybersecurity state and awareness. Perhaps, it is the reason why 80% of cyber incidents reported in Somalia target the government since they involve hacking government emails and web applications (Devi, 2017).

In this paper we also look at various cybersecurity controls that can be set up by the government of Somalia to minimize risk within the country and the different organisations.

7.3 Successful and unsuccessful areas of the study

Evaluating the cybersecurity state and awareness levels in Somalia's private and public sectors was mostly unsuccessful due to outdated literature. Most of the available literature was published more than three years ago or so and, therefore, does not contain accurate information. Somalia lacks processes for maintaining up-to-date information, such as catalogued cyber incidents within the past year, the most prevalent attacks in the private and public sector and implemented national cybersecurity policies for handling and responding to incidents.

As a result, it was challenging to understand the current true state of cybersecurity in the country. Fortunately, we were able to complete the evaluation successfully by combining the available data with the survey data to understand the contemporary cybersecurity state in Somalia. Since the focus of the research is to understand the current state of cybersecurity in the country, the study developed surveys capturing the most essential cybersecurity factors needed to understand the level of cybersecurity state and awareness in Somalia.

For the most part of the study targeted specific individuals, such as managers, C-level executives, and people working in institutions like NCA, with the questions since their input reflects the daily cybersecurity processes in their organizations. The survey data and synthesis of existing literature enabled us to understand the current cybersecurity situation in the country.

7.4 Existing limitations

Outdated Literature

The lack of updated literature explaining the cybersecurity situation in Somalia was a rife challenge during the study. We were often unable to access and collect accurate information regarding the current state of cybersecurity in Somalia as there is a lack of literature on this subject.

In the current body of literature, there is only one published research that looks into cybersecurity awareness in Somalia.

Research Methodology Limitations

Some of the C-suite executives were quite hesitant and not willing to participate in the study despite many efforts to encourage them to participate in the study. Respondents were slow to respond to the questionnaire in the first and second attempts, but third follow-up reminders were successful. Some respondents did not understand well the importance of the questionnaire.

7.5 Exploiting the results to address identified challenges

Primarily, the Somali government can exploit the results to strengthen the country's national cybersecurity position. Many of the results highlight the key challenges preventing Somalia from achieving a high level of cybersecurity, such as inadequate funding. The identification of what makes other countries successful in their cybersecurity implementation is important as Somalia can set up similar initiatives.

The government can opt for outsourcing cybersecurity functions to alleviate the costs and, at the same time, gain access to the best professionals and technologies in the cybersecurity industries. This and many other recommendations in the results can assist Somalia to provide adequate protection for its critical infrastructures.

Furthermore, the results indicated the lack of vital cybersecurity training and awareness among all the participants involved in the study. It implies that Somalia's private and public sectors lag behind in creating cyber awareness for members of the public as well as employees. For instance, a notable result is the lack of frequent

training as most people participating in the survey noted that their organizations have not conducted cybersecurity awareness and training for more than two years. By exploiting the results, relevant authorities can develop and implement cybersecurity awareness policies that require frequent training to increase awareness levels.

More importantly, the results have shown that Somalia lacks national cybersecurity guidelines, policies, and standards. The country has been left behind by most developing and developed nations that rely on acceptable cybersecurity standards to maintain robust cybersecurity. Therefore, the responsible authorities, including NCA and MPTT, can utilize the results to identify missing national cybersecurity policies and regulations and implement them.

Additionally, organizations in the private sector, including surveyed telecom companies and banks, can exploit the results to enhance their cybersecurity policies and procedures. Most of the survey questions purposed to evaluate the cybersecurity state by investigating aspects like the type of running security systems and implemented network security measures. For instance, a common trend identified across the surveyed sectors is a lack of fundamental cybersecurity measures, such as encryption, information backup operations, and managed or monitored firewall solutions.

Lastly, the relevant government agencies can exploit the results to identify lacking cybersecurity awareness among members of the public to inform the development and implementation of national cybersecurity awareness procedures. For example, the results show that most Somali residents are unaware of the best measures for protecting their devices. An aware and enlightened nation can enable Somalia to strengthen its cybersecurity position significantly.

7.6 Future work

An analysis of the survey results shows numerous areas for further development in the future. They include:

Cybersecurity Awareness and Training

Somalia lacks formal, defined processes for creating awareness and training individuals on cybersecurity best practices. Throughout the survey, it is clear that many organizations in Somalia have not conducted cybersecurity awareness and training processes for their employees for more than two years. While this is common in Somalia, cyber adversaries are always developing better techniques for executing malware, social engineering, or intrusion attacks.

The NCA and MPTT hence need to look into how they can develop national cybersecurity awareness and training frameworks requiring organizations to conduct mandatory training for their employees. Also, the authorities require to develop mechanisms for identifying training and awareness gaps in the public to ascertain that everyone has some level of cyber awareness.

On the same note, information security awareness focusing on best practices for securing digital information requires further development in Somalia. The majority of the people included in the survey stated that their organizations categorize information according to type but do not set specific access permissions. Also, the results illustrate that Somali organizations permit anyone to connect an external drive to office computers. These are poor cybersecurity measures that expose sensitive information to unauthorized access, modification, and exfiltration.

The Somali government in collaboration with players in the private sector require to identify and implement secure standards for securing information applicable across the divide.

Managed Cybersecurity

Managed cybersecurity is the most suitable alternative for governments or organizations lacking sufficient funds to invest in cutting-edge cybersecurity solutions capable of protecting against the current dynamic cyber threat landscape. However, the survey results indicate that the Somali government does not think much of outsourcing cybersecurity functions to reputable managed security providers. In this regard, the relevant authorities need to investigate how they can tap the benefits of

managed cybersecurity to gain access to lacking cybersecurity expertise and technologies.

Defence-In-Depth Approach

A defense-in-depth (DiD) approach leverages the security benefits of deploying multiple cyber defenses to make it extremely hard for attackers to hack a system or breach the security of sensitive information. However, the results show that majority of organizations do not implement defense-in-depth protection as most rely on traditional security systems.

Hence, defense-in-depth is among the areas requiring further development in the future. For example, the NCA can consider making it mandatory for all organizations handling sensitive information to implement a minimum of data protection controls, such as user access control, encryption, information/system backup, and frequent risk assessments.

Cyber Incidents Reporting Procedures

The survey results indicated that more than 80% of Somali organizations do no report cyber incidents or data breaches to the NCA. However, they cannot be blamed since Somalia lacks a national procedure for reporting cyber incidents. In this case, the responsible authorities are required to explore and identify a framework that requires mandatory reporting of cybersecurity incidents. This framework should include the development of a nationwide body headed by a data or privacy commissioner responsible for recording and investigating cyber incidents within the country.

7.7 Significance and contribution of the results

The broader significance of the study is it contributes to the overall enhancement of the cybersecurity positions and awareness in Somalia. The results have revealed a lack of sufficient cybersecurity awareness in the stakeholders and indicated a dire need for more cybersecurity procedures in the private and public institutions as well as general users.

By using the results of this study, the government and private entities can identify shortcomings in their cybersecurity preparedness as well as information security gaps. Therefore, the research makes an immense contribution in enabling the government to strengthen the security of its cyberspace.

8 Conclusions

The thesis's research objective was to study and evaluate cybersecurity awareness in Somalia and the challenges inhibiting the Somali government from achieving robust cybersecurity strategies. To achieve this aim, the research intended to meet the following objectives:

- Identify cybercrimes and threats.
- Analyse the current cybersecurity awareness in Somalia.
- Recognize best practices from several successful countries as well as from less developed countries.
- Provide recommendations on cybersecurity areas to be selected in future awareness campaigns.

A qualitative research methodology was used to achieve two of the four objectives mentioned above. By identifying cybercrimes and threats, we were able to understand the cybersecurity situation in Somalia, as well as in other countries. It also helped in guiding the topics used in the quantitative research. A quantitative research methodology comprising of surveys assisted in collecting required data from participants based in both the private and public sectors. An analysis of the survey results provided deep insights into the data, enabling the stated objectives' achievement. In the survey analysis chapter, it is clear the current cybersecurity state in Somalia is wanting.

There is a significant gap in how Somali citizens protect themselves from cyberattacks. The public awareness survey revealed that nearly half of the public population have not implemented any of the mentioned security measures to protect their devices. Further analysis showed that the internet penetration rate in

Somalia is still growing; hence most users are a novice and unable to protect themselves adequately from attacks. Additionally, the research showed that at least half of the population had encountered scams executed through emails, online games, and phones. It is an indication that social engineering attacks are rife in Somalia.

Another survey discovered that cyber awareness among public members is alarmingly low as the results indicated that 59.5% lack any cybersecurity awareness or training. For those with essential cyber awareness, 67.9% taught themselves, which is not an appropriate method for creating sufficient cybersecurity awareness.

A survey on bank institutions indicated that the current cybersecurity situation is not ideal for protecting sensitive information. A considerable number of people participating in the research revealed that they are not confident with their banks' cybersecurity status, while other expressed they are not sure if they are confident.

Cybersecurity in the private sector does not meet the recommended levels. For example, the research discovered that most banks and telecom organizations use traditional, unmonitored, and unmanaged antivirus/firewall, and intrusion detection appliances while neglecting necessary controls, such as encryption and information/system backup operations. As such, they are unable to achieve the highest possible level of cybersecurity protection.

A government survey also showed that the main challenge preventing the Somali government from improving its cybersecurity state is inadequate funding and an acute shortage of skilled cybersecurity professionals. Since the government does not outsource any cybersecurity functions, it is apparent that the cybersecurity state will remain at undesirable levels.

The result reflects one of the core cybersecurity challenges affecting the government's ability to deliver robust cyber protection, which is a dire lack of public cybersecurity awareness. The same issue persists in the private sector. A survey done on banks and organizations in the telecom sectors showed that employees were last exposed to cybersecurity awareness and training programs more than two years ago. With staff members waiting long periods to participate in refresher cybersecurity

training programs, they may be unaware of recent threats and recommended cybersecurity practices for preventing data breaches and attacks.

On the same note, phishing and vishing attacks are the most common in the banking division and second most common in the telecom industry, which further shows the risks of a poorly trained and unaware workforce. One of the notable results in the banking sector is the lack of formal regulatory banking structures and complicated relationships between the legal systems. The lack of regulatory banking structures prevents the government from resolving conflicts, such as transaction scams, further inhibiting the banking industry from achieving healthy cybersecurity measures.

Also, a common trend noted in both the banking and telecom industry is that most entities' information security programs lack written policies, plans and guidelines for securing critical systems and information. Further, a large number of survey respondents indicated that their banks lack business associate agreements with third-parties with access to sensitive information; the same goes to the telecom companies.

A resounding 70.3% of participants from government agencies like the NCA and MPTT stated that the government is yet to develop national cybersecurity standards and strategies. In comparison, an overwhelming 91.3% indicated that the government had not implemented a single national cybersecurity standard. It is a clear indication of a low level of implementing cybersecurity policies and strategies in Somalia's private and public sectors.

We encountered several limitations during the research, which are expounded in detail in the discussion chapter. In a nutshell, the main limitations of this study include:

- At the present body of literature, there is only one published research paper that looks into cybersecurity awareness in Somalia.

- The targeted executive-level managers were quite hesitant and not willing to participate in the study notwithstanding many efforts to encourage them to participate in the study. Respondents were slow to respond to the

questionnaire in the first and second attempts, but third follow-up reminders were successful. Some respondents did not understand well the importance of the questionnaire.

References

Abhishek Kumar, A. M. 2015. A Review of Security and Data Hiding Techniques. International Journal of Inventive Engineering and Sciences (IJIES), 31.

Ahmed Yousuf Jama, M. M. 2015. Survey on Data Modification Attacks. International Journal of Scientific & Engineering Research, Volume 6, Issue 2, 778-781.

Aker C., Mbiti M. 2010. Mobile Phones and Economic Development in Africa, Journal of Economic Perspectives.

Allan Friedman, P. W. 2013. Cybersecurity and Cyberwar: What Everyone Needs to Know.

Anderson. 2001. Why Information Security is Hard. An Economic Perspective. Annual Computer Security Applications Conference.

Arnold, R. 2017. Cybersecurity: A Business Solution: An executive perspective on managing cyber risk.

Ashford, W. 2018. Retrieved from Economic impact of cybercrime is significant and rising: Retrieved from https://www.computerweekly.com/news/252435439/Economic-impact-of-cyber-crime-is-significant-and-rising

Augenbaum, S. 2019. The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime.

Australian Government. 2020. Australia's Cyber Security Strategy 2020.

Australia's Cyber Security Strategy. 2016. Australia.

Bashir, H. 2019. Cyber Security in Somalia.

Becker, G. 1968. Crime and Punishment: An Economic Approach. Journal of Political Economy Vol.76, No. 2, 169-177.

Boston Consulting Group. 2015. The internet economy in the G20.

Broadhurst, R. 2006. Developments in the global law enforcement of cybercrime. Policing, 29(3), 408–433. Retrieved from https://doi.org/10.1108/13639510610684674

Broadhurst, R. 2006. Developments in the global law enforcement of cybercrime.

Brotherston, A. B. 2017. Defensive Security Handbook: Best Practices for Securing Infrastructure.

Burnette, M. 2020. Three Tenets of Information Security. Retrieved from https://www.lbmc.com/blog/three-tenets-of-information-security/#:~:text=The%20fundamental%20principles%20(tenets)%20of,are%20called%20the%20CIA%20Triad.

Bussell, J. 2013. Britannica. Retrieved from https://www.britannica.com/topic/cyberspace

CERT-Somalia 2018. Retrieved from http://som-cert.org/about-us/

Chubb. 2019. The Importance of Cybersecurity in Business. BBC.

Cisco. 2020. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

Combat Cyber Crime, 2014. Department of Homeland Security.

CSIRO. 2018. Cyber Security A Roadmap to enable growth opportunities for Australia.

David, W. 2008. Cybercrime, media and insecurity: The shaping of public perceptions of Cybercrime. International Review of Law Computers and Technology, 45-63.

Devi, A. 2017. Cyber Crime and Cyber Security, 160–171. Retrieved From https://doi.org/10.4018/978-1-5225-2154-9.ch011

Ewan Sutherland. 2017. Governance of Cybersecurity – The Case of South Africa, University of the Witwatersrand (Wits), Johannesburg.

Flaherty, A. 2013. House Passes Pro-Business Cybersecurity Bill. Claims Journal.

Forum, I. S. 2011. Cyber Security Strategy. Information Security Publication.

Gagliardone, I., & Sambuli, N. 2015. Cyber Security And Cyber Resilience In East Africa.

GCI. 2018. Global Cybersecurity Index (GCI), USA: ITU.

Gibson, W. 1984. Neuromancer.

Halpern, J. 2010. Helpernadvisers. Retrieved from https://www.halpernadvisors.com/why-is-confidentiality-important/

Hankin, C. 2017. Cyber Security – Defend, Deter and Develop.

Hare, H. 2007. ICT in Education in Somalia, SURVEY OF ICT AND EDUCATION IN AFRICA: Somalia Country Report.

Homeland Security. 2020. DHS. Retrieved from https://www.dhs.gov/topic/cybersecurity

Hope, C. 2020. Computer Hope. Retrieved from https://www.computerhope.com/jargon/u/unauacce.htm#:~:text=Unauthorized%20access%20is%20when%20someone,it%20is%20considered%20unauthorized%20access.

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

ITU. 2018. Global Cybersecurity Index 2018. ITU, 16.

Jidka Warshaddaha. 2019. A Survey on Cyber Security awareness among university students in Mogadishu.

Kaspersky. 2020. Kaspersky Security Bulletin 2020. Statistics. Retrieved from https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

Kemp, S. 2020. Datareportal. Retrieved from https://datareportal.com/reports/digital-2020-somalia

Krishnaswamy, K. N. 2016. Management Research Methodlogy: Integration of Principles, Medthods and Techniques. New Delhi: Pearson Education India..

Kshetri, N. 2013. Cybercrime and cybersecurity in the global South. Basingstoke, U.K: Palgrave Macmillan.

Kshetri, N. 2019. Cybercrime and Cybersecurity in Africa. Retrieved from Journal of Global Information Technology Management: https://doi.org/10.1080/1097198X.2019.1603527

Lancaster, H. 2018. Somalia - Telecoms, Mobile and Broadband - Statistics and Analyses. BuddeComm.

Lebied, M. 2018. A Guide To The Methods, Benefits & Problems of The Interpretation of Data. Retrieved from https://www.datapine.com/blog/data-interpretation-methods-benefits-problems/

Little, P. 2003. Somalia: Economy without State. Indiana University Press.

Lord, N. 2018. What is Insider Data Theft. Data Theft Definition, Statistics and Prevention Tips. Retrieved from https://digitalguardian.com/blog/what-insider-data-theft-data-theft-definition-statistics-and-prevention-tips

Menon, S. 2013. Our dependence upon cyberspace. India.

Michael E. Whitman, H. J. 2011. Principles of Information Security.

Monica Lagazio, N. S. 2014. A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, online, (pp. 1-32).

National Cyber Security Programme UK Government. 2016. Britain's Cyber Security Bolstered by World Class Strategy.

National Strategy. 2014. Mauritius National Cyber Security Strategy, First edn.

Norton. 2011. Norton Cybercrime Report. Norton Inc.

Office Cabinet. 2009. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.

Penicaud C., & McGrath, F. 2014. Innovative Inclusion: How Telesom ZAAD Brought Mobile Money to Somaliland. GSMA Mobile Money for the Unbanked Programme.

Ponemon Institute for IBM. 2016. Cost of Data Breach Study.

Rapid7. 2020. Brute force and Dictionary Attacks. Retrieved from https://www.rapid7.com/fundamentals/types-of-attacks/

Rapid7. 2020. Common Types of Cybersecurity Attacks. Retrieved from https://www.rapid7.com/fundamentals/types-of-attacks/

Republic of Rwanda, National Cyber Security Strategy. 2015. Republic of Rwanda, Kigali.

Richard A. Clarke, R. K. 2019. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.

Richmond, R. 2012. A Seven-Step Guide to Protecting Customer Privacy. Retrieved from https://www.entrepreneur.com/article/222552

Ross Anderson, C. B. 2012. Measuring the Cost of Cybercrime. Proceedings of the 11th Workshop on the Economics of Information Security (WEIS).

Rouse, M. 2019. Retrieved from: https://searchwindevelopment.techtarget.com/definition/Internet

Rout, S. 2008. Network Interferences. Retrieved from http://www.santoshraut.com/forensic/cybercrime.html

Sachkov I. 2017. Targeted attacks on banks. Russia as a testing ground

Saini, H. R. 2012. Cyber-Crimes and their Impacts: A Review. International Journal of Engineering Research and Applications (IJERA), 202-209.

Sambuli, N., & Gagliardone, I. 2015. Cyber Security and Cyber Resilience in East Africa. London: Centre for International Governance Innovation and Chatham House.

Saunders, M., Lewis, P. & Thornhill, A. P. 2009. Research Methods for Business Students. 5th, ed. Rev. ed. Essex: Pearson.

Senate Canada. 2018. The Standing Senate Committee on Banking, Trade and Commerce.

Smith, A. D. 2004. Cybercriminal impacts on online business and consumer confidence. pp. 224-234.

Statista. 2018. Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2018. Retrieved from

https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/

Steele, J. 2019. creditcards.com. Retrieved from https://www.creditcards.com/credit-card-news/payment-method-statistics-1276/

Strategy. 2017. National Cybersecurity Strategy, Arab Republic of Egypt: Cybersecurity Council.

Stremlau, N. 2012. Somalia: Media law in the absence of a state. International Journal of Media & Cultural Politics.

Swami, S. 2017. Aryaka. Retrieved from https://www.aryaka.com/blog/network-disruption-here-is-how-to-stop-it/#:~:text=Traditionally%2C%20network%20disruption%20was%20a,%2C%20backup%20links%2C%20and%20failovers

Symantec. 2016. Cyber Crime & Cyber Security Trends In Africa. Refrieved from https://thegfce.org/cybercrime-and-cybersecurity-trends-in-africa/

The Heritage Foundation. 2020. 2020 index of Economic Freedom.

The News Tribune. 2014. Power Grid Shockingly Vulnerable to Cyberterrorism.

Thomson et al. 2006. A conceptual framework for cyber-security awareness and education in SA

Tunggal, A. T. 2020. Retrieved from https://www.upguard.com/blog/information-security

U.S. H.R. 3523. 2012. Permanent Select Committee on Intelligence. U.S. House of Representatives

U.S. H.R. 624. 2011. Cyber Intelligence Sharing and Protection Act. U.S, U.S.

UN; Economic Commission for Africa. 2014. Tackling the challenges of cyber-security in Africa; policy brief. Retrieved from https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

Unwin, P. 2009. Introduction. In T. Unwin, Information and communication technology for development (pp. 1-6). Cambridge: Cambridge University Press.

Venkat, H. 2016. Retrieved from CYBER CRIME: http://alphasquadblogging.blogspot.com/2016/12/virus-dissemination-for-past-few-days.html

Waldman, A. E. 2018. Privacy as Trust: Information Privacy for an Information Age.

Woodford, C. 2020. Retrieved from https://www.explainthatstuff.com/internet.html

Wright, C. 2019. How Cyber Security Can Protect Your Business: A guide for all stakeholders.

Young, S. 2016. Britain to Spend 1.9 Billion Pounds on Boosting Cyber Defences. Reuters.

Appendices

Appendix 1. Public Awareness Survey

1. Which of the following reasons do you use the Internet? Please select all appropriate options.
   -Multiple-choice checkbox with the following choices:
   *To run business
   *To browse news

*Emails or social media
*Online banking/ Money Transfer
*For studies or research

2. How often do you use online /mobile money banking? Please select only one options.
   -Radio button with the following choices:
   *Twice a week or more
   *Once a week
   *Twice a month
   *Once a month
   *Occasionally
   *Rarely
   *Never

3. How/where did you learn about cybersecurity? Please select all the appropriate options.
   -Multiple-choice checkbox with the following choices:
   *University, college, etc
   *Workplace training
   *self-taught
   *Do not know anything about it

4. What kind of security measures have you taken personally?
   -Multiple-choice checkbox with the following choices:
   *Take backups regularly
   *Use multiple passwords for each account
   * Avoid opening email/attachments from unknown sources
   *Avoid posting personal information on the Internet
   *None of the above

5. Do you have antivirus installed on your device?
   -Radio button with the following choices:
   *Yes
   *No
   *I don't know

6. How often do you update applications on your device?
   -Radio button with the following choices:
   *It is done automatically
   *At least twice a month
   *At least once a month
   *Occasionally, when I remember
   *When I am reminded by the application
   * When I am reminded by my software
   * Never

7. With the use of the Internet, have you encountered such problems as given below in the past two years? Please select all the appropriate options below.

-Multiple-choice checkbox with the following choices:
*Intentional or accidental leakage of business/company information
*Scams done through phone/emails/online games
*Unauthorized access
*Virus or malware attack
*None of the above
*I don't know

Appendix 2. Bank Institutions Survey

1. How confident are you in your bank overall cyber security position? Rate from 1 to 5 where 5 is extremely confident and 1 is not at all confident.
   -Radio button with the following choices:
   *1
   *2
   *3
   *4
   *5

2. Which of the following security measures are implemented in your bank? Please select all the appropriate options below.
   -Multiple-choice checkbox with the following choices:
   *Anti-virus/Firewall protection
   *Intrusion Detection System
   *Backup operations
   *Encrypt confidential information
   *None of above

3. What kind of antivirus solution does your bank use?
   -Radio button with the following choices:
   *Managed/monitored antivirus and gateway UTM solution
   *Monitored antivirus managed by an IT service provider
   *Monitored antivirus solution managed from a company's central server
   *Paid-for version of standalone antivirus, unmanaged & unmonitored
   *The free, unmanaged/unmonitored antivirus is used on all systems

4. What level of security has been implemented within your bank to separate different kinds of information (financial, legal, HR, etc.) and access to it?
   -Radio button with the following choices:
   *Everyone can access all bank's data
   *Data is organized by type, but no specific permissions have been set
   *Data is organized by type, and staff is allowed access based on user need for each type
   *No security or management

5. Who is allowed to connect external drivers to their office computers?
   -Radio button with the following choices:
   *Only authorized members of the staff using a company-owned external drive on certain computers

*Any staff member, but only drives provided by the company, after a virus scan runs
*Any staff
*Anyone

6. When was the last time your bank conducted an information security awareness training program for employees?
   -Radio button with the following choices:
   *More than 2 years ago
   *One year ago
   *6 months ago
   *3 months ago (or less than 3 months ago)
   *Never conducted any security assessment

7. Does your cybersecurity program include drafted policies, plans, and guidelines for securing, managing, and monitoring the following systems or programs? Please select all the appropriate options below.
   -Multiple-choice checkbox with the following choices:
   *Core banking system
   *Security devices such as firewall(s) and proxy devices
   *Remote access connectivity
   *Portable devices such as PDAs, laptops, cell phones, etc.
   *Breach incident response plan
   *Identity theft prevention program
   *None of them

8. Has your bank experienced any of the following cyberattacks in the past 12 months? Please select all the appropriate options below.
   -Multiple-choice checkbox with the following choices:
   *Computer virus and/or Malware
   *Unauthorized user accessing customer/company data
   *Phishing and/or Vishing
   *DDoS attack (A distributed denial-of-service)
   *I have not experienced a cyberattack
   *I don’t know

9. Have you encountered any material security incidents concerning the customers in the past two years?
   -Radio button with the following choices:
   *Yes
   *No

10. Are identified cyber incidents reported to NCA (The National Communications Authority) or MPTT (Ministry of Post, Telecommunications and Technology, Somalia)?
    -Radio button with the following choices:
    *Yes
    *No

11. Does your bank work with third parties, such as IT service providers, that have access to your information?
    -Radio button with the following choices:
    *Yes
    *No

12. Do you have a baseline or any other security requirements for third parties that must be considered? (Applicable if "Yes" is selected in the above question)
    -Radio button with the following choices:
    *Yes
    *No

Appendix 3. Telecom Institutions Survey

1. How confident are you in your organization's overall cybersecurity position? Rate from 1 to 5 where 5 is extremely confident and 1 is not at all confident.
   -Radio button with the following choices:
   *1
   *2
   *3
   *4
   *5

2. Which of the following security measures are implemented in your bank? Please select all the appropriate options below.
   -Multiple-choice checkbox with the following choices:
   *Anti-virus/Firewall protection
   *Intrusion Detection System
   *Backup operations
   *Secure Wireless Access Points
   *Encrypt confidential information
   *None of above

3. What level of security has been implemented within your organisation to separate different kinds of information (financial, legal, HR, etc.) and access to it?
   -Radio button with the following choices:
   *Everyone can access all company's data
   *Data is organized by type, but no specific permissions have been set
   *Data is organized by type, and staff is allowed access based on user need for each type
   *No security or management

4. What level and/or type of Internet/web filtering is being used by your organization? (UTM devices inspect Internet traffic for viruses, spam, and website requests and filter malicious content).
   -Radio button with the following choices:
   *Maximum: UTM appliance only allows users to visit approved web sites

*Medium: Antivirus software on the computer systems block users from infected
*Minimal: Employees are told what websites are acceptable
*None: Web browsing is not restricted, monitored or filtered in any way

5. Is User Access Control (UAC) turned on for the workstations within your organization?
-Radio button with the following choices:
*Turned on for all computer systems, and it requires an Administrator to approve changes
*Turned on for all computer systems, but staff can click past it
*Turned on for a few systems, but not all of them
*Not turned on for any computer system

6. Who is allowed to connect their personal devices to your wireless network connection? (Cellphones, laptops, tablets, etc.)
-Radio button with the following choices:
*No one is allowed to connect personal devices to our wireless network
*Connect only to a dedicated Guest Access wireless connection, with a guest passcode
*Connect only to a dedicated Guest Access wireless connection, without a passcode
*Only people who we give the encryption passcode can connect
*Anyone: it doesn't require any passcode to connect to it

7. Who is allowed to connect external drives to their office computers?
-Radio button with the following choices:
*Only authorized members of the staff using a company-owned external drive on certain computers
*Any staff member, but only drives provided by the company, after a virus scan runs
*Anyone, work related, after their antivirus performs a mandatory virus scan
*Anyone, as long as it is work related
*Anyone can connect their external drives

8. Does your organization have any of the following written policies and/or procedures? Please select all the appropriate options below.
-Multiple-choice checkbox with the following choices:
*Customer and employee information privacy policy
*Network security policy
*Breach incident response plan
*Business continuity/disaster recovery plan
*Workstation use policy
*None of the above

9. When was the last time your organization conducted an information security awareness training program for employees?
-Radio button with the following choices:
*More than 2 years ago

*One year ago
*6 months ago
*3 months ago (or less than 3 months ago)
*Never conducted

10. Does your organization work with third parties, such as IT service providers, that have access to your information?
    -Radio button with the following choices:
    *Yes
    *No

11. Do you have a baseline or any other security requirements for third parties that must be considered? (Applicable if yes is selected in the above question).
    -Radio button with the following choices:
    *Yes
    *No

12. Does your company experience any of the following cyberattacks in the past 12 months? Please select all the appropriate options below.
    -Multiple-choice checkbox with the following choices:
    *Virus and malware attack
    *Phishing and/or vishing attacks
    *Ransomware attack
    *Denial of Service (DoS) attacks
    *Advanced Persistent Threats (APT)
    *I don't know

13. Are identified cyber incidents reported to NCA (The National Communications Authority) or MPTT (Ministry of Post, Telecommunications, and Technology)?
    -Radio button with the following choices:
    *Yes
    *No

Appendix 4. Government Institutions Survey

1. Which of the following is a barrier for Somali government to achieve the highest possible level of cybersecurity?
   -Radio button with the following choices:
   *Inability to pay competitive salaries for cybersecurity personnel
   *Insufficient number of cybersecurity staff
   *Lack of funding for cybersecurity infrastructure
   *Security situation in the country
   *Lack of adequately trained cybersecurity personnel
   *Lack of end user accountability
   *All of above

2. Does the government outsource any of its cybersecurity functions?
   -Radio button with the following choices:
   *Yes

*No
*I don't know

3. Has the government implemented national cybersecurity policy, standards, and strategy plan?
   -Radio button with the following choices:
   *Yes
   *No
   *I don't know

4. Has the government implemented national cybersecurity policy, standards, and strategy plan?
   -Radio button with the following choices:
   *Yes
   *No
   *I don't know

5. Do you have a system or procedure to catalogue and count attacks, incidents, and breaches?
   -Radio button with the following choices:
   *Yes
   *No
   *I don't know

6. Is the government able to determine the types of attacks and have the capacity to countermeasure?
   -Radio button with the following choices:
   *Yes
   *No
   *Not sure

7. How frequently does the government take any of the following actions to improve its cybersecurity practice?
   a) Risk assessment
      -Radio button with the following choices:
      *Never
      *Monthly
      *At least quarterly
      *At least annually
      *At least every 2 years
      *Do not know

   b) Technical security review
      -Radio button with the following choices:
      *Never
      *Monthly
      *At least quarterly
      *At least annually
      *At least every 2 years

*Don’t know

c) Forensics services after incidents or breaches
-Radio button with the following choices:
*Never
*Monthly
*At least quarterly
*At least annually
*At least every 2 years
*Don’t know

d) Cybersecurity staff training
-Radio button with the following choices:
*Never
*Monthly
*At least quarterly
*At least annually
*At least every 2 years
*Do not know