**UNIVERSITY OF NAIROBI**

**SCHOOL OF COMPUTING & INFORMATICS**

# FACTORS AFFECTING INFORMATION SECURITY IN TELEWORKING. CASE STUDY: KENYA NATIONAL POLICE DT SACCO


**BY:**

**JESEE KAMAU WACHIRA**

**P54/34955/2019**

**SUPERVISOR**

**DR. EVANS MIRITI**


**A research project presented in partial fulfillment of the requirement for the award of MSC. Information Technology Management in the School of Computing and Informatics, University of Nairobi**

**SEPTEMBER 2021**

# DECLARATION

I declare that this is my original project and has not been presented for a degree in any other university.

Signature  Date ……August 17, 2021…….

**WACHIRA JESEE KAMAU: P54/34955/2019**

This project has been submitted for presentation with my approval as the University Supervisor:

Signature  Date 17-08-2021 …….

**DR. EVAN K. MIRITI**

**School of Computing and Informatics**

**University of Nairobi**

## ACKNOWLEDGEMENT

I acknowledge the support accorded to me by my supervisor, Dr. Evan Miriti without whom I could not have gone this far with my project. You have tirelessly walked the entire journey with me to the completion of this research work. Thank you.

My gratitude goes to the staff of Kenya National Police DT SACCO who took their time and effort to provide me with the data necessary to complete this research work. Thank you very much.

To the University of Nairobi school of computing and informatics, for the opportunity given to me to do this study, and to all the lecturers who contributed in my quest for knowledge, receive my gratitude.

To my fellow students in the school of computing and informatics, friends, and colleagues who encouraged me through the journey, I appreciate your contributions.

## DEDICATION

This project paper is dedicated to my family, friends, and my colleagues at Kenya National Police DT SACCO who kept me going for their great inspiration, never-ending encouragement, and prayers towards the successful completion of this course.

Am grateful to God for giving me the strength and resources to walk through this long journey.

## ABSTRACT

Businesses are increasingly adopting teleworking to embrace the changes in the operation macro environment, the COVID 19 pandemic is driving most businesses to adopt teleworking to curb its spread, and teleworking is gradually becoming the new norm, however, attackers globally are taking advantage to launch large-scale attacks such as phishing and computer-based exploits. This study looks at ways of ensuring that teleworking is adopted in a secure way to avoid any form of breach of data security. The research objectives were to identify the ICT security risks related to teleworking, identify the human behavior likely to lead to an information security breach, and propose the controls necessary to combat information security risk. The study adopted the general deterrence theory and the theory of perceived behavior. The study used mixed research methods guided by a cross-sectional survey design. A cross-sectional design was used in formulating the hypothesis and testing the relationship between the variables. The study targeted the employees of the Kenya National Police DT SACCO where a sample size of 42 was adopted. The study established that Kenya National Police DT SACCO has adopted teleworking and has taken the necessary security measures to enable teleworking. The study recommends that the organization should look at the 17.9% of people who have not undertaken any information security training and train them on the same. Information security is also a highly dynamic field where changes and challenges evolve every day and hence there is a need for continuous training and review of the information security policy. There is a need to look at the type of access to systems given to people who telework and should be limited to only the resources that they need to run their day-to-day activities and access should not be left open but only granted on need be as and when required. There is a need to monitor any anomaly behavior. Teleworking may also act as a staff backup plan to achieve business continuity in case of calamity that affects an organization, the staff teleworking will be spared. There is a need to develop technologies to identify employees working from home using security software to identify the employees biometrically.

## Table of Contents

**Abbreviations and Acronyms**

ICT- Information and Communication Technology

IT- Information Technology

COVID- Corona Virus Disease

GDPR – General Data Protection Regulation

EU- European Union

Wi-Fi- Wireless Fidelity

ILO- International Labor Organization

FOSA- Front Office Service Activity

SACCO- Savings and Credit Cooperative Organization

ISO- International Organization for Standardization

GDT- General Deterrence Theory

BOYD- Bring Your Own Device

VPN- Virtual Private Network

DT- Deposit Taking

VAPT- Vulnerability assessment and penetration testing

**List of Figures**

List of Tables:

# CHAPTER ONE: INTRODUCTION

## 1.1Background to the study

Employees work from home / outside the office (remotely) through the internet and related technologies, this is also known as teleworking, the employees gain access to data and applications hosted on corporate servers. Teleworking is not an emerging trend, it was initially attributed to the oil crisis of the 1970s (Tammy D, 2015). In the wake of Corona Virus Disease COVID-19, it has rebounded as a measure to safeguard people from coronavirus disease (Covid -19). Most companies have permitted their employees to work away from the traditional office either from home or other locations (Angel B 2020). Robert A. (2013) highlights that with the advancements in technology and availability of enabling infrastructure; it is becoming increasingly easy and affordable for employees to work away from the office. Robert A. (2013) argues that without a reliable internet connection telework is impossible. Many internet service providers have made it possible to have affordable internet connections and stable power sources, Laptops and other mobile devices like tablets have become affordable to the users (Ernest and Young 2008). A lot of emphasis is given to the economic and social benefits of teleworking but little concern is given to security, many organizations are happy about the job being done as normal but forget to look at the information security concerns (Diana F, 2020). There is a need to review the different issues related to information security in teleworking.

Companies and the government have been urged to be more careful in matters of data protection and as a result, in November 2019 Kenya enacted a Data Protection ACT 2019. Others countries across the globe have laws on data protection e.g. GDPR – General Data Protection Regulation, which is a regulation issued by the European Commission to strengthen and unify data protection for individuals within the EU.

## 1.2 Problem Statement

Breach of data security taints a company's reputation and consumers, as well as potential investors, shy away, it is therefore very crucial for an organization to focus on privacy and security (Juma'ah A, 2020). Kenneth (2020) observes that as COVID -19 compels more employees to work from home and stay connected to office resources, attackers globally are taking advantage to launch large-scale attacks e.g. phishing and computer-based exploits.

There is also the challenge of employers monitoring the employee's activities while working from home (James P, 2011). Despite teleworking posing a risk, there is limited attention being taken to mitigate the risk as opposed to other risks. There is a lack of prescribed policies in functioning procedures or preparation in place to inform employees around the risk of data loss or alleviate the risk of breach of privacy and security concerning personal information.

According to ISO IEC 27002, security processes should be put in place to protect information retrieved, processed, or kept at teleworking sites. The policy should define the conditions and restrictions for using teleworking. The policy looks should look at the measures taken at the teleworking site to enhance physical security, the communication security in the remote access protocol, and the sensitivity of the information transmitted. According to the standard, other persons using the accommodation pose a threat of unauthorized access to information or resources. The standard looks at a possibility of disputes on intellectual property rights concerning developments on privately-owned equipment. There is also the danger of litigation issues while accessing privately-owned equipment during an investigation, the use of personal computers also increases the risk of data loss. There are few controls deployed in identifying employees such as security software and biometric identification of employees working from home. James P (2011) points out that remote locations may lack physical security and the data processing in systems and

applications can cause information security threats different from those of an office setup. According to Scott (2020), some organizations have also failed to evolve IT Security to match the growth in teleworking they lack the security tools to secure the workforce and also require IT security policy training.

## 1.3 Research objectives

To identify the ICT security risks related to teleworking

To identify the human behavior likely to lead to a breach of information security

To propose the controls necessary to combat information security risk

## 1.4 Significance of the study

This study hopes to come up with ways of ensuring that teleworking which is a form of working that is gaining popularity in many sectors is adopted in a secure way to avoid any form of breach of data security. The study aims at looking at other factors of security apart from availability, integrity, and confidentiality. The study will contribute to filling gaps identified by other researchers in areas of information security.

# CHAPTER TWO: LITERATURE REVIEW

## 2.1 Introduction

This chapter highlights a review of literature on teleworking with a view of providing an informed background in regards to the research objectives. A review of the three major facets of security is done, the research further looks at other factors affecting information security and comes up with an information security framework combining several factors. The research looks at human behavior concerning technology, organization, and environment and how they affect information security threats in addition to those defined by the information security triad. According to the American National Security Telecommunications and Information Systems Security Committee (NSTISSC), Information Security defends information, the organization's facilities and systems that store, use and transmit information from threats to preserve the value it gives to an organization. The fundamental principles of security are confidentiality, integrity, and availability which should be safeguarded at all times. Confidentiality ensures essential levels of secrecy are enforced while processing data and avoid unauthorized disclosure. Confidentiality is enforced for data at rest and in transit. The integrity of data is the guarantee of accuracy and reliability of information and systems from unauthorized modification. Availability is defined as reliability and timely access to data and resources to only authorized individuals.

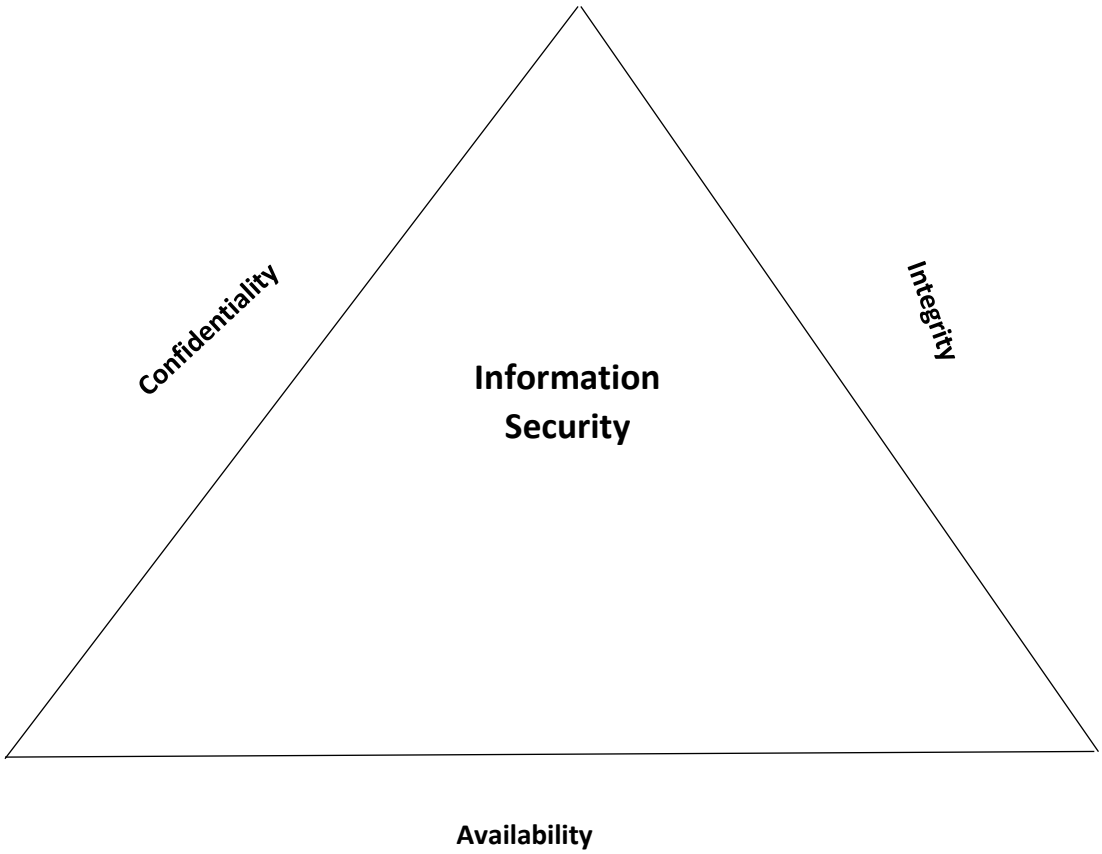


Figure 1.1

Information Security Triad. Source: NIST

## 2.2 Teleworking overview

According to the International Labor Organization (ILO), telework is defined as the use of Information and Communications Technologies (ICTs), such as smartphones, tablets, laptops, and/or desktop computers, for work that is performed outside the employer's premises. A literature review is necessary to understand information security threats in teleworking environment, the organizations allowing teleworking need to implement security measures and both formal and informal controls. According to International Labour Office (2016), the increase in good infrastructure and stable internet has made it possible for companies to take advantage of

teleworking. With the increased cases of COVID 19 and restrictions to movements, most organizations have allowed employees to work from home. Information security is critical to the success of teleworking.

Peter J (2011) defines teleworking as work practice involving remote computing conducted predominately from homes and occasionally from organized telecentres. Teleworking uses information and communication technology (ICT) to allow employees to work and relate virtually with colleagues and customers without physical presence within a period of time. Teleworking is not restricted to only working from home but from any setting that is conducive to support ICT.

According to ISO IEC 27002, teleworking is any forms of work outside of the office, including telecommuting, flexible place of work, remote work, and virtual work environments.

## 2.3 Teleworking security issues

Stewart (2015), defines risk as to the likelihood that a threat will exploit a vulnerability causing harm to an asset. It assesses the probability, possibility, or chance. The higher the likelihood that a threat event will occur, the greater the risk. Every exposure instance is a risk.

Ampomah(2013) notes that despite the many benefits such as cost reduction and maintaining a green environment there are teleworking challenges associated with information security based on information integrity, availability, and confidentiality, especially where employees are required to access highly classified and sensitive information. He notes that various strategies have been introduced to address information security such as authentication, access controls, data compartmentalization, encryptions, and layered defense/ defense in depth. Despite the much literature on applying security strategies to teleworking, protecting classified information in teleworking remains a challenge.

ISO IEC 27002 requires the implementation of a policy and supporting security measures to protect information accessed, processed, or stored at teleworking sites. The policy should define the conditions and restrictions for using teleworking. The policy looks should look at the physical security measures taken at the teleworking site, the communication security in the remote access protocol, and the sensitivity of the information transmitted. According to the standard, other persons using the accommodation pose a threat of unauthorized access to information or resources. The standard looks at a possibility of disputes on intellectual property rights concerning developments on privately-owned equipment. There is also the danger of litigation issues while accessing privately-owned equipment during an investigation, use of personal computers also increase the risk of data loss.

Kenneth (2020) notes that the current wave of teleworking has not been scheduled or planned but has rather occurred as an emergency and been necessitated by the rise in COVID-19 and the efforts to control it, the emergency situation has created a unique security challenge that needs to be closely monitored and controlled. The major security concerns of an employee working remotely are convenience, privacy and safe computing, the company data transmitted across networks need to be protected and sensitive documents shared among legitimate participants. To improve on security several factors are taken to consideration such as preventive controls, proper setup of the system and avoiding factory default settings, running updates, and fully patching of systems. Kenneth (2020) recommends the use of fully-featured cloud services, using secure means to share virtual meeting links, and use of secure meeting ID with controlled sessions having a waiting room and lock meeting feature.

Information security involves, people, technology, and processes, information security is the accidental or intentional disclosure, modification, or destruction of information, it is subdivided

into availability, confidentiality, and integrity, a breach of any of these results in information security. Breach to Information confidentiality occurs when data at rest or in transit is accessed and read by unauthorized parties. Information integrity breach is the modification of the intended meaning of information by unauthorized persons. Information availability breach is the inaccessibility of information to an authorized person, which is likely to be caused by a denial-of-service attack.

Apart from breach of confidentiality, integrity, and availability scholars have examined other security issues regarding teleworking, which can be categorized as people, physical equipment (technology), organization, and environment Ampomah(2013) this research will examine the human behavior in technology, organization and environment and the effect they have in information security.

### 2.3.1 People / human factor in information security

Human factor are the environmental, organizational, work factors and human and personal characteristics that influence human behavior. According to Jeimy (2019), people are regarded as the weakest link in a security chain and notwithstanding all the technical measures and security procedures, people have the highest possibility of exposing organizations to vulnerabilities. Alavi (2016) observes that human factors and influence create a great challenge for information security systems as they often make inconsistent and subjective decisions that pose a great risk to information assets. Human factor poses a security threat to information security, they suffer from social engineering attack which is used by attackers to access classified data. Human factors are related with organizational culture and personal perceptions and characteristics. Aleksandar (2019) notes that employees pose a potential information risk through such vectors like passwords, computer users select passwords that are simple and to remember or those passwords that relate to

their personal data, users still share passwords with their colleagues or write them in visible places or fail to change them over a long period of time. A lot of training and awareness is necessary to change this behavior. In addition to the training, awareness, and education provided to people, sanctions are defined for behaviors that go against the security procedures and processes for safeguarding information, but despite all the measures put in place people still perpetuate vulnerabilities either due to error, acts of omission, or deliberate actions that puts an organization's sensitive information at risk of exposure. Henry (2018) notes that significant budgetary expenditures are set for cybersecurity tools but there is little effort in the human factor and organizations' security culture.

### 2.3.2 Technology factor in information security

According to Angel (2020) technology is a significant aspect in development of teleworking as teleworking rides on technical infrastructure. The evolving computational technology brings about a lot of advantages such as accessibility and availability of resources for organizations however this brings a new security challenge and risk. According to Morrison (2019) the computer systems within an organization, the rate of fault-tolerance of the systems, and the degree of redundancy as well as the cybersecurity measures deployed impact the uptake of teleworking. Organizations use different means of communication, such as allowing employees to use personal emails in official communication, Aleksandar (2019) emphasizes the use of corporate email address which is controlled by the institution and where all necessary security requirements are met. Ernest and Young report (2008) points that most organizations lack privacy-enhancing tools which are crucial in telecommuting setups such as biometric identification and controls and the capability to enforce compliance as well as monitoring.

### 2.3.3 Organizational factor in information security

An organization's policy may allow or discourage teleworking, where the policy allows for teleworking, the organization faces a different kind of risk. A risk is defined as asset containing a vulnerability exploitable by a threat. According to Yang (2013), organizations that allow teleworking lead expose the organization to different vulnerabilities that would result in data security risk including information disclosure, modification, and destruction. Githinji (2014) observes that in Kenya the people who can telework are only those with laptops and have access to the internet, managers also make the decision of who can telework and those that cannot telework based on the nature of work. According to NIST (2009), the major security concerns for organizations allowing teleworking and remote access are absence of physical security controls at the teleworking sites, the use of networks that may be insecure, infected devices connecting to internal networks, and internal resources being available to external hosts.

### 2.3.4 Environment factor in information security

According to a report by Ernest and Young (2008) most organizations fail to perform periodic audits of telecommuter’s physical working environment, the organization may require employees to have a clean desk policy in the office but this may be hard to implement for employees teleworking. According to Mugwika (2016), penetration of mobile and internet in Kenya stands at 83% and 58% respectively making it among the highest in Africa. Kenya is ranked position 21 globally as the most connected population to the internet with 26.1 million internet users. Kenneth (2020) emphasizes the need for a stable network connection as quality degradation could impact the output and potentially diminish the systems integrity and cybersecurity rating. According to the Kenya Power website and daily notifications on local dailies to customers, there are daily schedules of planned power interruptions, this, in turn, affects teleworking.

This research is going to look at how human behavior in relation to technology, organization, and environment affect the information security of teleworkers and the necessary measures required to safeguard the teleworker and the organization's information.

## 2.4 Theoretical Framework.

According to Sommestad (2013), the behavior of employees significantly affects information security. An information security policy is mainly developed to guide employees on the good practice of ensuring information is secured. The policy sets guidelines for compliance and describes repercussion for non-compliance and security policy violation, the acceptable and non-acceptable use of computer resources, the expected conduct regarding information security, and defines the necessary training required by the employees. It is paramount for employees to know what is required of them to avoid any instances of an information security breach. Information security has been a concern for many years and a lot of researchers have used different theories to analyze and understand the concept, this research paper will analyze the Theory of Planned Behavior and General Deterrence Theory. Godlove (2011) states that it's necessary to understand how teleworkers' approaches are related to their readiness to comply with set guidelines and uphold data security in the telework setting.

### 2.4.1 Theory of planned behavior

According to the theory of planned behavior by Ajzen (1988), the paramount prediction of behavior is obtained by asking people if they are intending to conduct themselves in a certain way, the theory assumes that consumers make a decision by weighing the cost and benefits of different courses of actions and opting for the option that capitalize on their expected net benefit. In making the decision it is assumed that the consumer has access to adequate information to make informed decision.

### 2.4.2 General Deterrence Theory (GDT)

General Deterrence Theory (GDT); the theory possess that an individual's behavior can be altered through the use of perceived punishments. According to D'Arcy (2011), Deterrence theory is one of the most broadly applied theories in research on information systems security, mainly within behavioral information systems security studies. The organizations use perceived punishments that are defined actions the organization thinks are needed to alter the behavior. These actions can be defined in organization policies and this will define the desired and undesired behaviors, it looks at how employees either comply or fail to comply with policies and abuse or misuse of information system resources. General deterrence theory has been used to envisage a user behavior that can either be loyal or disruptive of information systems security. The general deterrence theory assumes that people make logical decisions towards perpetration or refraining from crime based on the fully realization of their benefits and cost (D'Arcy et al, 2011).

As a theoretical foundation, the GDT will be used to examine how the organization's policies, the organization's technology, and infrastructure as well as the users surrounding environment affects teleworking. A well-developed system with necessary system controls increases the chances of detecting computer abuses. Other factors likely to determine an employee's behavior towards information security would be his position and opportunities in the role and the traits of the works that moderate the general deterrence theory (D'Arcy et al, 2011). In teleworking an employee is mainly de-individualized from the other employees, according to de-individualization theory which is the psychological separation of individuals from others, people have a greater inclination to perceive themselves as detached from responsibilities for their actions enabling deviant behaviors. According to Schuessler (2009) resources poverty may hinder the implementation of information security breach countermeasures, timely identification of relevant threats, and

effective management of the systems. This research will be based on the theory of Deterrence behavior.

## 2.5 Conceptual Framework.

This section describes the conceptual framework developed by this research. The conceptual framework is founded on the following variable: technology, organizational, and environment as the independent variables, and information security as the dependent variable. The conceptual framework seeks to show the relationship between teleworking and information security threats.

Bernik (2016) points out that gauging information security performance helps an organization determine the degree to which their security requirements are met. The effectiveness of information security can be measured by different ways ranging from the level at which compliance to the best practices is attained, how a company has established and enforced a data security policy, and the extent to which employees are equipped with the right tools and technologies. Information security is also affected by personal devices within a network, therefore the extent to which BOYD is regulated and the measures are taken to ensure security compliance to network security requirements for the BOYD can be used to measure effectiveness on information security, both the BOYD and corporate devices should be checked for current and up to date patches. Teleworking requires the use of internet connections and the source and connection to the internet should be secured and instituting a zero-trust approach for all connections. For a deeper analysis of the effectiveness of information security Bernik (2016) talks about vulnerability assessment and penetration testing (VAPT), risk analysis and return on investment justifications.

The conceptual framework is represented in Figure 2.1

Conceptual Framework; Human behavior that determine the security of information by teleworkers

Independent Variables

Dependent variable

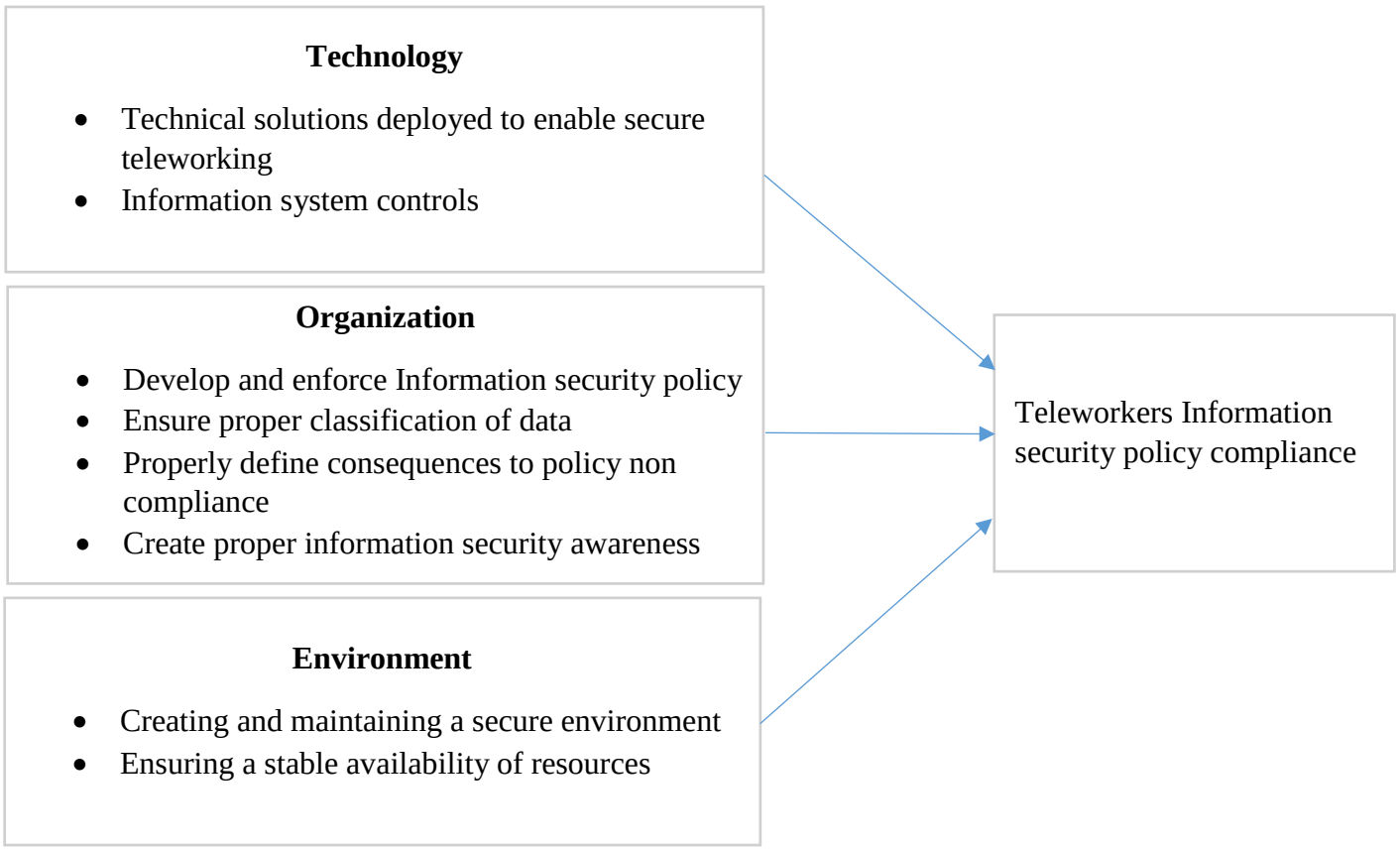


Figure 2.1: Conceptual framework

Source; Adapted from General Deterrence Theory (2011)

## 2.6 Operationalization of Variables;

Williamson (2016) defines operationalization as a process of removing vagueness in written work and research where definition of all relevant variables is done. The variable is measured so that it can be stated and expressed quantitatively or qualitatively.

Operationalization of variables table;

| Variable | Type of Variable measurement | Indicators |
|---|---|---|
| Technology | Source of internet (Categorical) | Availability of stable internet connection |
| | | Availability of internet connection backup e.g. modem |
| | Source of power (nominal) | Availability of stable power source<br>Availability of power backup solution |
| | Device protection (nominal) | Disk Encryption<br>USB Device control<br>Device loss |
| | | Malware/ virus attack |
| | | |
| | Secure technologies used in connection (categorical) | Use of VPN<br>Restrictions to unsecure public connections protocols<br>Session monitoring and recording |
| | | |

| | | |
|---|---|---|
| | | Use of professional and licensed tools like MS Teams and GTalk<br>Multi-level Authentication and user identity management. |
| Organization | Organization support in teleworking (Categorical)<br><br>Training and awareness in teleworking (Categorical)<br><br>Type of access while teleworking (Categorical)<br><br>Policy on Information Security | Provide enabling technology e.g. Laptops, modems and phones<br>Approval for teleworking requests<br><br>Training intervals<br><br>Frequency of teleworking e.g. Daily, weekly, monthly, working hours (8am to 5pm) or rarely<br>Allowing access on personal devices.<br><br>Availability of Policy on Information Security - ease of access to the document, ease of understanding the document, ease of clarification from the ICT security staff. |
| Environment | Stability of resources e.g. power and internet (Categorical) | Internet link uptime<br>Power stability |

| | | |
|---|---|---|
| | | Mobile phone talk time allocated |
| | Availability of secluded home office (Nominal) | Availability of home office/ teleworking station |
| | Other home occupants in the SACCO industry (Nominal) | Possibility of sharing devices with other members in the family |
| Teleworkers Information security policy compliance | Information Security Policy Document. (Nominal) | Availability of Information Security Policy- ease of access to the document, ease of understanding the document, ease of clarification from the ICT security staff. |
| | | How often the document is reviewed. |
| | | The consequences for non-compliance |

# CHAPTER THREE: RESEARCH METHODOLOGY

## 3.1 Introduction

This chapter defines the research design and the methodology that was used in the study. It highlights, research design, population, sample size and sampling technique, data collection instruments, data collection process, measurement and scaling techniques, data analysis and processing, statistical method and hypothesis testing.

## 3.2 Research Design

This study used mixed methods research guided by a cross-sectional survey design. Cross sectional design was used in formulating the hypothesis and testing the relationship between the variables (Kothari, 2004). A cross-sectional survey gathers data to make inferences around a population of interest (universe) at one point in time. Surveys are excellent vehicles for collecting original data for studying the attitudes and orientations of a population. This study outlined the activities that were done from the point of formulating hypothesis to data analysis.

## 3.3 Population of the Study

Kenya Police SACCO has a workforce of 122 employees, it has it's headquarter in Nairobi and seven branches across the country. The population of interest will be from the headquarter (Nairobi) and the branches namely, Kisii, Kakamega, Nyeri, Eldoret, Mombasa, Meru and Nakuru. The study will target staff from the different departments within the SACCO namely, Accounts, FOSA, Procurement, Records, Investment Department, Audit, Risk and compliance, Credit, Marketing, Human Resource and Administration, top management and the ICT. The population is a mix of people from different levels of management and geographical locations. This research will include all departments both ICT and non-ICT related staff, it will also sample vendors and services providers offering remote support. This research will look at employees who utilize

teleworking from the different departments. Majority of the sample size utilize teleworking apart from a few functions that cannot be performed remotely e.g FOSA services. Teleworking is also done on rotational basis in the institution, that is working from the office a few weeks and teleworking a few weeks. According to Hamed (2016) it is doubtful that researchers must be able to collect data from all cases thus there is need to select a sample.

Snowball sampling method was used; snowball sampling is an approach that uses recommendations to find possible respondents with the specific range of traits in this case, these are the employees that work from home, it is useful to a particular subject, snowball sampling was used due to its simplicity in reaching the intended respondents.

**Table 3.1: Categories and Number of respondents**

| **Category** | **Population** | **Sample size** |
|---|---|---|
| Senior management | 4 | 2 |
| Accounts Department | 15 | 3 |
| Marketing and customer care | 11 | 2 |
| FOSA | 8 | 4 |
| Credit department | 13 | 3 |
| Records Department | 5 | 3 |
| Audit, Risk and Compliance Department | 5 | 2 |
| Human Resource and Administration | 16 | 3 |
| Procurement | 2 | 1 |
| ICT | 6 | 3 |
| Investment Department | 3 | 2 |
| Kisii Branch | 5 | 2 |
| Meru Branch | 5 | 2 |
| Eldoret Branch | 5 | 2 |
| Mombasa Branch | 5 | 2 |
| Nyeri Branch | 5 | 2 |
| Kakamega Branch | 5 | 2 |
| Nakuru Branch | 5 | 2 |
| **Total** | **122** | **42** |

## 3.4 Data Collection Instrument

Both primary and secondary data were collected. Primary data was collected from the respondents willing to participate in the study, using a structured questionnaire to allow for descriptive analysis from the responses. Secondary data was gathered from reading materials such as published journals in information security, this guided in examining the already existing risks in information security.

Piloting was done to ensure that the questionnaire is free from vagueness and the data generated is implicitly analyzed in relation to the stated research objectives. This was done by administering the questionnaire to a few staff; in branches with similar characteristics as the study respondents. After piloting, alterations were made in order to address any areas of concern. Permission to collect data was sought from the General Manager ICT and Business Innovations' office.

## 3.5 Data Analysis and Processing

The data collected using questionnaires were edited, coded, and entered into MS Excel for data analysis. The study implemented both descriptive and inferential statistics. The questionnaires used in data collection had both open-ended and close-ended questions. Google forms were used to create the questionnaires, this aided in the easy distribution of the questionnaire and avoid physical forms that may be a hazard during these COVID times. The Google forms also aided in data analysis by presenting the results in pie charts and bar graphs. The open-ended questions produced qualitative data, which was categorized according to research objectives; these were mainly be reported in narrative formats. The close-ended questions provided the quantitative data to be presented in tables and graphs. Descriptive statistics delivered summaries around the sample and the measures and formed a basis for the analysis of quantitative data.

The research used descriptive statistics such measure of central tendency – mean, measures of variability (standard deviation) and measure of relative frequencies.

# CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

## 4.1 Introduction

This chapter consists of the research findings, data analysis, presentation, and interpretation. The responses were analyzed in line with the objectives and in different sections from the demographic data, the targeted population understanding of information security, the technological factor, the level of risk related to organizational factor, and the level of risk related to the environment.

## 4.1 The Human aspect in information security.

From the questionnaire distributed to the participants there was 92.86 percent response. Pie chart 1, shows the characteristics of the participants who answered the questions from the questionnaire distributed. 7.7 % of them have been working in the SACCO for over 15 years, 12.8% have been working in the SACCO for 10- 15 years, 43.6% have been working in the SACCO for 5 – 10 years and 35.9% have been working in the SACCO for less than 5 years.

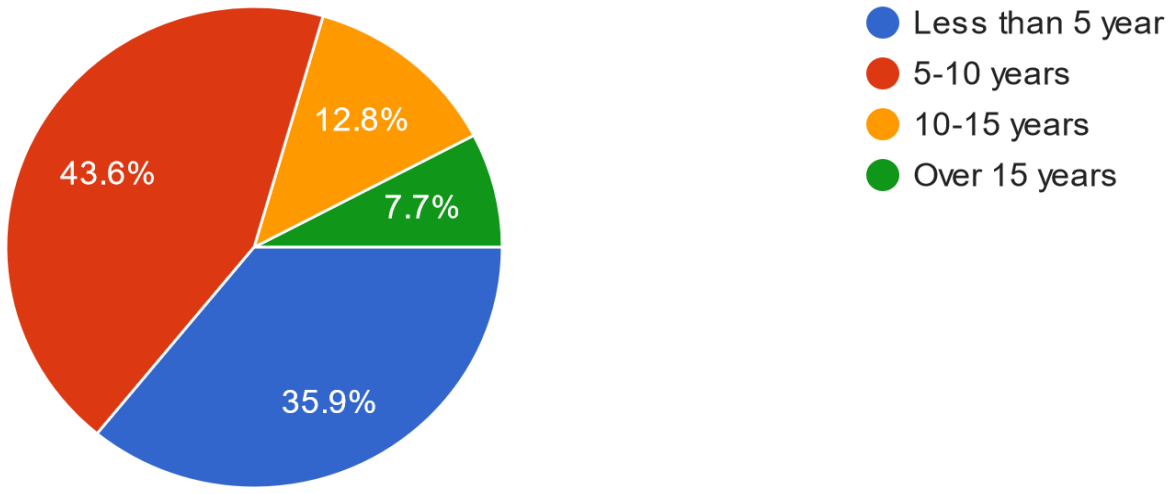


Figure 4.1: Participants years in the SACCO

| | Not at all | Small Extent | Moderate Extent | Great Extent | Very Great Extent | Mean | Std Dev |
|---|---|---|---|---|---|---|---|
| Understanding information Security | 0% | 2.6% | 41% | 46.2% | 10.3% | 3.64 | 0.71 |
| Undertaken Training in information Security | 17.9% | 35.9% | 28.2% | 17.9% | 0% | 2.46 | 0.99 |
| Have home offices | 15.4% | 20.5% | 28.2% | 25.6% | 10.3% | 2.9 | 1.25 |
| People in SACCOs | 28.2% | 33.3% | 17.9% | 17.9% | 2.6% | 2.33 | 1.15 |

Table 4.1: Participants characteristics.

From the respondents' responses in table 4.1, it is clear that a majority of the employees understand information security, despite some of them having not undertaken any training on information security none of the respondents does not understand information security. 97.4 % of the population have an understanding of information security. However, there is a small group of 2.6 percent that have a very small understanding of security and 17.9 % who have not undertaken any training in information security posing a risk to information security and need to be trained.

A conducive working environment is necessary for the success of teleworking, however, 15.4% of the population do not have what can be termed as a private space or home office to work from and another 20.5 % enjoy home office while teleworking to a very small extent. The remaining group enjoys the home office with 2.6% enjoying a home office fully. Working from home may lead to industrial espionage especially where the people around you work in the same sector, around 38.4 % of the respondents have people who work in other SACCOs around them while working from home, while the rest have no people in the SACCO industry around them while working remotely.

## 4.2 The technology aspect in information security

The participants were asked about technological factors that are likely to lead to breach of information security such as insecure source of internet

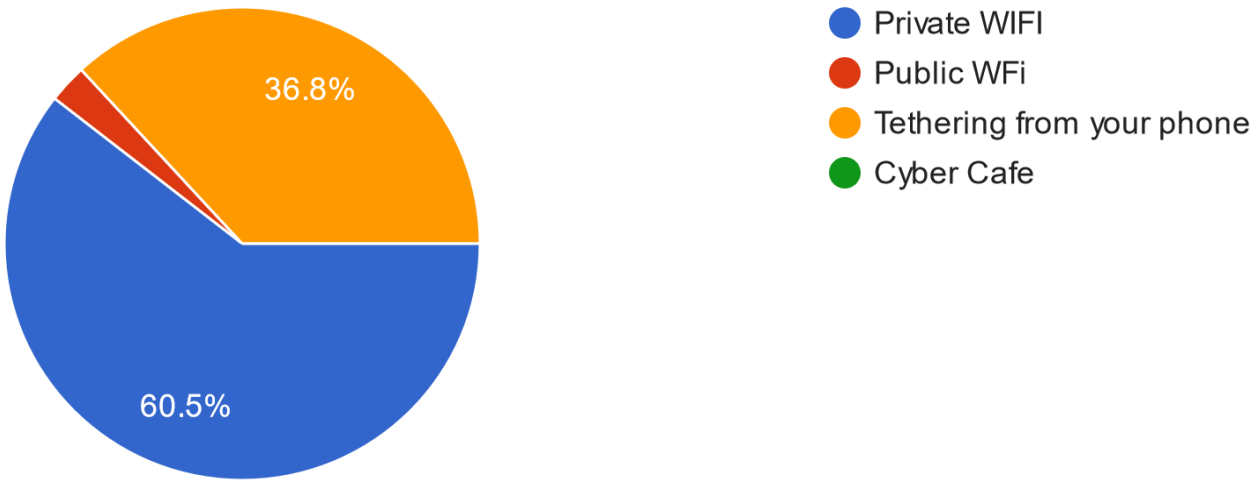


Figure4.2: Source of internet while teleworking.

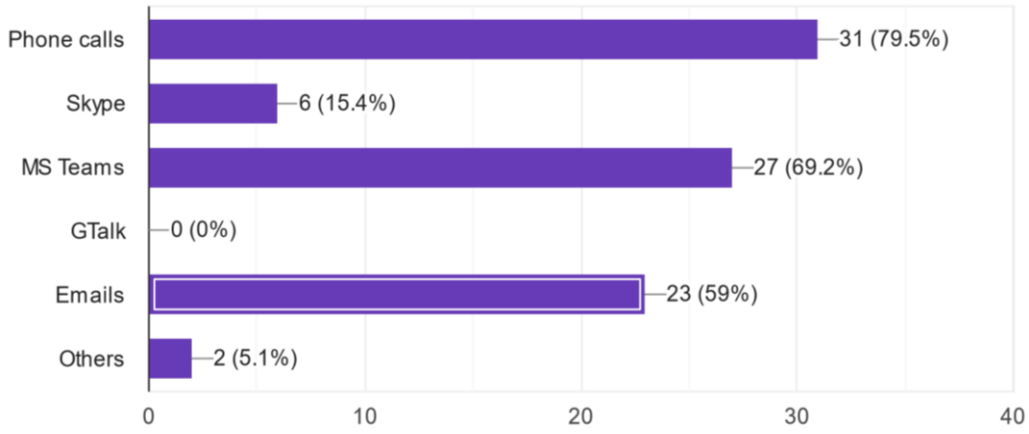


Figure 4.3: Mode of communication.

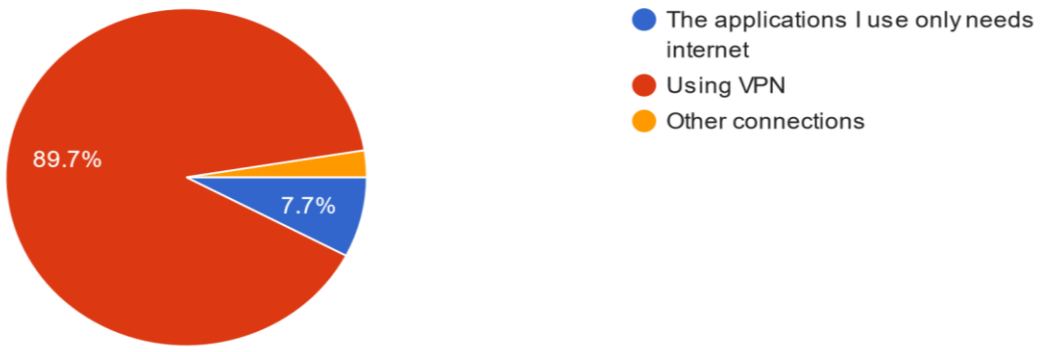


Figure 4.4: Mode of connecting to office network.

| | Yes | No |
|---|---|---|
| Disk Encryption | 84.6% | 15.4% |
| Credentials used (Domain (yes) Local (no)) | 92.3% | 7.7% |
| Device loss | 2.6% | 97.4% |
| Data Transfer | 10.3% | 89.7% |
| Data Loss | 7.7% | 92.3% |
| Malware attack | 2.6% | 97.4% |
| Use of personal device | 81.6% | 18.4% |

Table 4.2: Technology controls in place.

From the employees' responses, it's clear that the technology aspect of information has been put in place to deter employees from possible components that may lead to information insecurity, the employees majorly use private Wi-Fi at 60.5 % and tethering from their phones at 36.8 % for their internet source. Communication with other employees in the office or working from home is mainly through phone calls and Microsoft Teams as well as emails, a few indicated use of WhatsApp Messenger for communication.

A secure platform is used in accessing company resources, that is through the use of VPN at 89.7% with a few employees working on only internet-facing applications at 7.7 % and local machines applications like Microsoft Excel and Microsoft Word at 2.6%.

The ICT department has also taken necessary measures to ensure that the right technology solutions have been deployed to protect the employees from possible information security breach incidents. Restrictions on the endpoint have been implemented and employees are not allowed to use personal devices in teleworking. A few employees at 18.4% indicated the use of personal

devices on responding to emails. The organization has also laid down the necessary infrastructure for the network and ICT security staff to have visibility of who is teleworking and what they are doing.

### 4.3 The organizational aspect in information security.

We further looked at the organizational aspect in support of information security, this sought to understand the level at which the organization has put the necessary measures to ensure corporate information is secure while teleworking. The organization has an information security policy that is annually updated and easily accessible to the employees.

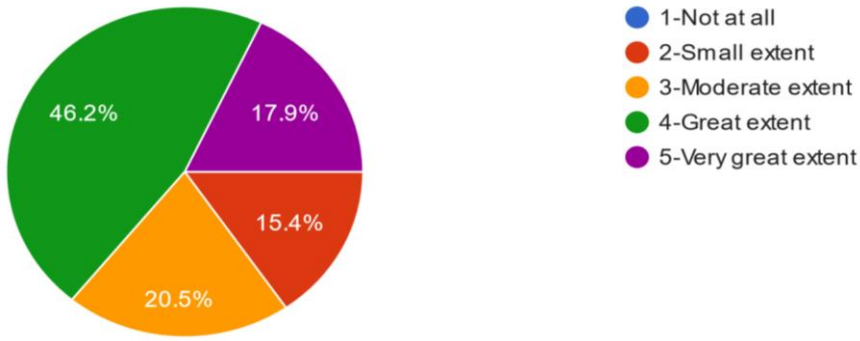


Figure 4.5: Extent that the organization supports teleworking.

A good number of employees at 84.6 % felt that the organization supports them in teleworking, organization support in teleworking is a key component to its success as they put the right policies to govern the process.

| | Yes | No |
|---|---|---|
| Understood information security policy | 89.7% | 10.3% |
| Read information security policy | 86.8% | 13.2% |
| Understood the consequences of noncompliance to information security policy. | 94.7% | 5.3% |

Table 4.3. Information security Policy

From the respondents, 86.8 % of the targeted employees have read the information security policy and understood it, they also indicated that they knew the consequences of noncompliance to the policy which deterred them from behaviors that may cause information security breach.


Figure 4.6: Type of access to systems while teleworking

All employees have restricted access to the systems while teleworking and access to the systems is only given on request when required this mainly happens during working days. However, staff from ICT have full access for support purposes.

## 4.4 The environmental aspect in information security

The environmental aspect of information security are factors that may information security breach such as in availability of systems while teleworking. The major components here while teleworking are power and internet down time.

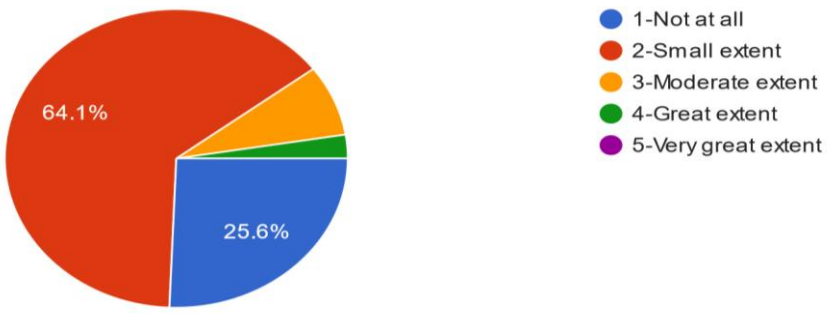


Figure 4.7. Power outage while teleworking

Majority of employees at 92.7% do not face power outage that may cause them not to proceed with their normal operations during teleworking. 38.5 % of the employees have a power backup plan, although a majority of employees at 61.5% do not have a power backup plan, they rarely fail to telework due to power failure.

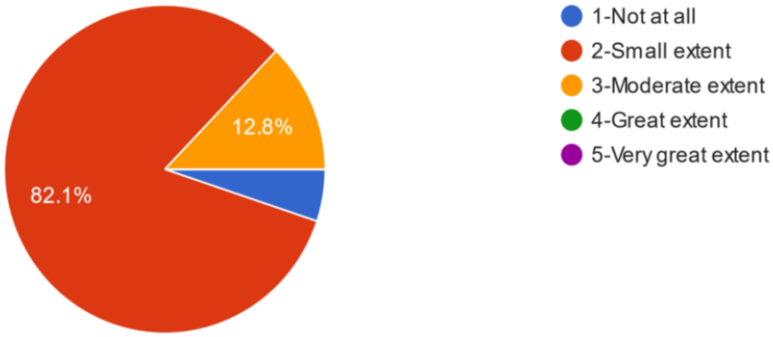


Figure 4.8: Internet outage while teleworking

94.9 % of employees do not suffer from internet outage and may be seen to have a stable internet source. A majority of them at 64.1% indicated that they had a backup for internet source. Only 35% do not do not have a backup for internet.

# CHAPTER 5 SUMMARY, CONCLUSION AND RECOMMENDATIONS

## 5.1 Introduction

The chapter looks at the significance of the research findings in relation to the research objectives on the factors affecting information security in teleworking at Kenya National Police DT SACCO. The chapter further discusses conclusions and recommendations.

## 5. 2 Summary

The main purpose of the study was to look at the security posture of teleworking at the Kenya National Police DT SACCO, identify the employees' behavior in relation to technology, organization policies, and the teleworking environment that are likely to impact information security. The research established that a considerable number of employees had embraced teleworking at the Kenya National Police DT SACCO, it also found that the organization had developed different mechanisms to allow employees to telework.

General Deterrence Theory (GDT) possess that an individual's behavior can be altered through the use of perceived punishments. The organization has an information security policy that as per the research findings most employees have read and understood and the documents are also reviewed annually. The organization has further implemented different tools and information security measures to deter employees from engaging in activities that may breach information security, such as denying them from copying data from removable devices and use of personal computers while teleworking. Access to systems is also limited and given on a need basis.

The research was also looking at the information security concerns in teleworking, it sought to understand the employees' behavior in relation to technology, organization policy, and teleworking environment. The research found out that a majority of the Kenya National Police DT SACCO staff who undertake teleworking understood information security, a few had undertaken

training in information security, it further found out that the organization had an information security policy that was easily available to the staff as a majority of the respondents had read the policy. The organization had also put down the necessary infrastructure and technology to allow the employees to work remotely and securely.

The majority of the staff who worked from home lacked home offices and the working environment was not office-friendly with only 35.9 % of the employees enjoy a home office, there were also 38.4% of staff who lived with people that work in the SACCO industry.

## 5.3 Conclusion

The research sought to identify the factors affecting information security in teleworking at the Kenya National Police DT SACCO, these factors are likely to affect other organizations in the SACCO sector and other financial institutions. The research identified that lack of home offices and working from home with people who are also in the same sector may lead to industrial espionage. The research also found out the organization needs to come up with the necessary information security policy that is well understood by the people that are going to work from home in order to guard the safety of the information being shared. The organization also needs to come up with the necessary enabling infrastructure for teleworking.

## 5.4 Recommendation

The organization should look at the 17.9% of employees who responded and have not undertaken any information security training and train them on the same. Information security is a highly dynamic field where changes and challenges evolve every day and hence there is a need for continuous training and review of the policy on information security.

The information accessed, processed and stored at teleworking sites should be secured, this includes the physical security of the teleworking location and the communication security in the

remote access protocols, secure protocols such as VPN should be enforced, there is also need to look at the sensitivity of information being transmitted.

There is need to look at the type of access to systems given to people who telework and should be limited to only the resources that they need to run their day-to-day activities and access should not be left open but only granted on need be as and when required and monitor any anomaly behavior.

Employees should also be assisted to buy cost-efficient power backup solutions to aid them in having an uninterrupted working session when working from home.

Teleworking may also act as a staff backup plan where in case of calamity that affects an organization, those working from home may be lucky to be safe this will work as a business continuity plan.

There is a need to develop technologies to identify employees working from home using security software to identify the employees biometrically.

## 5.5 Limitation of the study

Information security is a sensitive area to touch on and especially where there is recorded evidence of responses, there was a general lack of cooperation from the respondents as they felt maybe the information shared would be used against them, some respondents also thought the questionnaire was from malicious sources and had to confirm it's source severally before proceeding despite the researcher approaching them in advance to request them to respond to the questionnaire. Additionally, some aspects of information security are too sensitive to be shared openly in a questionnaire.

There was also a lack of information from the respondents as some did not have broad exposure in the field of information security while some did not fully understand some technical jargon.

## 5.6 Areas of further research

Further study can be done on factors affecting information security in teleworking other than the ones stated in this research. Further research can be conducted on the information security posture for organizations that allow for teleworking against those that do not allow for teleworking to understand whether information security risk is higher or lower in either the organizations that allow teleworking or those that do not allow teleworking. Research should also be done to establish how business functions that are not technology-driven can benefit from teleworking, such functions as hospitality.

References


1. K. Okereafor and P. Manny, "Solving Cybersecurity Challenges of Telecommuting and Video conferencing application in the Covid-19 pandemic*" International Journal in IT & Engineering (IJITE)* vol. 8, issue 6, pp 5-10, 2020.
2. Robert A (2013) "The Influence of Information Technology on Telework: The Experiences of Teleworkers and Their Non-Teleworking Colleagues in a French Public Administration" International *Journal of Information and Education Technology, Vol. 3, No. 1,*
3. Peter J. (2011) "Are existing security models suitable for teleworking." *Australian Information security management Conference*
4. Juma'ah, A. and Alnsour, Y. "The Effect of Data Breaches on Company Performance*" International Journal of Accounting and Information Management (IJAIM). Vol. 28, no. 2, 2020*
5. *Challenges and opportunities of teleworking for workers and employers in the ICTS and financial services sectors:* Issues paper for the Global Dialogue Forum on the Challenges and Opportunities of Teleworking for Workers and Employers in the ICTS and Financial Services Sectors (Geneva, 24–26 October 2016), International Labour Office, Sectoral Policies Department, Geneva, ILO, 2016.
6. D Jorge (2020) "Key consideration for ensuring the security of organization data and information in teleworking from home" *Researchgate journals*.
7. Scott G (2020) "Security workers beyond the perimeter" *Researchgate journals.*
8. Angel B (2020) "Teleworking in the Context of the Covid-19 Crisis" doi:10.3390/su12093662
9. James, P. (2011). Are existing security models suitable for teleworking? DOI: https://doi.org/10.4225/75/57b533efcd8c0

10. Diana F. et al (2020)" Big Data and the Ethical Implications of Data Privacy in Higher Education Research" DOI: 10.3390/su12208744
11. ISO IEC 27002 (2013) Information Technology- security techniques- code of practice for information security controls. Second edition.
12. Ernest Young (2008) "Risk at home, privacy and security risks in telecommuting." Centre for Democracy Technology,
13. Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, Manjeera. (2013). Security risksin teleworking: a review and analysis. Melbourne, The University of Melbourne
14. Githinji Ruth (2014) Telecommuting System for Kenyan organizations.
15. Ampomah M. Et al (2013) *Information Security Strategy and Teleworking security*
16. Angel Belzunegui (2020) *Teleworking in the context of the Covid-19 crisis*
17. Aleksandar Erceg (2019) *Information security: threat from employees.*
18. Reza Alavi (2016) A risk driven investment model for analyzing human factors in information security.
19. Kothari, C. R. (2004). Research Methodology: Methods and Techniques (2nd ed.). New Delhi: New Age International limited
20. Steward JM. Et al (2015) Certified Information Systems Security Professional Study Guide
21. Hamed Taherdoost. Sampling Methods in Research Methodology; How to Choose a Sampling Tech- nique for Research. International Journal of Academic Research in Management (IJARM), 2016, 5. hal-02546796
22. Henry W (2018) Human factors in information security culture: A literature review
23. Jeimy J. The human factor in information security. ISACA Journal (2019) volume 5
24. Williamson G. (2016) Operationalizing variables.

25. Tammy D (2015) How effective is telecommuting? Assessing the status of our scientific findings.
26. Joseph H (2009) General Deterrence Theory; Assessing information systems security effectiveness in large vs small businesses.
27. Morrison Joseph Et al (2019) Factors that influence Information Technology Workers' Intention to telework: A South African Perspective.
28. D'Arcy et al, (2011) A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings
29. Sommestad et al, (2013) A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance.
30. Mugwika (2016) Telecommuting model for small and medium enterprises (SMEs) in Kenya
31. Bernik (2016) Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation
32. Godlove (2019) Examination of the factors that influence teleworkers' willingness to comply with information security guidelines

# APPENDICES

## Appendix I: Questionnaire

Available online as: https://docs.google.com/forms/d/1NnkeughAou8p-rrp03IwsLKtW0EU92ZbI6yHposC8Cs/edit

This questionnaire is aimed at collecting data required for a study on the assessment of factors affecting security in data teleworking. Your participation in this research is highly treasured and you are kindly requested to complete the questionnaire. Kindly note the information you provide will be used for academic purposes and will be treated with utmost confidentiality.

**Section 1: SECTION 1: Demographic data**

1. What is your position/title in the organization?

   _____

2. How long have you worked with Kenya National Police DT SACCO?

   Less than 5 year [ ] 5-10 years [ ] 10-15 years [ ] Over 15 years [ ]

**Section 2: Levels of risk exposure (people related).**

3. To what extent do you understand information security? Use the scale of 1 to 5 where,

   1-Not at all [ ]

   2-Small extent [ ]

   3-Moderate extent [ ]

   4-Great extent [ ]

   5-Very great extent [ ].

4. Have you undertaken any training on information security in regards to teleworking? Use the scale of 1 to 5 where,

1-Not at all [ ]

2-Small extent [ ]

3-Moderate extent [ ]

4-Great extent [ ]

5-Very great extent [ ].

5. When working remotely to what extent do you work alone and in private? Use the scale of 1 to 5 where,

   1-Not at all [ ]

   2-Small extent [ ]

   3-Moderate extent [ ]

   4-Great extent [ ]

   5-Very great extent [ ]

6. To what extent do people that you relate with during teleworking work in SACCO, Use the scale of 1 to 5 where,

   1-Not at all [ ]

   2-Small extent [ ]

   3-Moderate extent [ ]

   4-Great extent [ ]

   5-Very great extent [ ].

**Levels of risk exposure (Technology Related)**

7. What is your source of internet when teleworking?
    a) Private WIFI [ ]
    b) Public WIFI [ ]
    c) Tethering from your phone [ ]
    d) Cyber cafe [ ]

8. Is your laptop hard disk encrypted? YES [ ] NO [ ] (tick appropriately)
9. Which credentials do you use to connect remotely? Domain credentials [ ] Local Credentials [ ] (tick appropriately)
10. Have you lost your mobile devices e.g. Laptops while teleworking? YES [ ] NO [ ] (tick appropriately)
11. Are you allowed to move data between your devices using removable devices e.g. flash disks? YES [ ] NO [ ] (tick appropriately)
12. Have you lost data through loss of laptop or removable devices e.g flash disks? YES [ ] NO [ ] (tick appropriately)
13. Has any of your device been affected by a malware while working remotely? YES [ ] NO [ ] (tick appropriately)
14. Do you ever work from personal devices e.g Laptops while teleworking? YES [ ] NO [ ] (tick appropriately)
15. How do you connect to the office network while working remotely?
    a) The applications I use only needs internet [ ]
    b) Using VPN [ ]

**c)** Other connections [ ] Specify_____

16. How do you communicate to people in the office?

a) Phone calls

b) Skype

c) MS Teams

d) GTalks

**Levels of risk exposure (organizational related)**

17. To what extent do you think the organization supports you in teleworking?

Use the scale of 1 to 5 where,

1-Not at all [ ]

2-Small extent [ ]

3-Moderate extent [ ]

4-Great extent [ ]

5-Very great extent [ ].

18. How often do you telework?

a. Every day of the week [ ]

b. Twice a week [ ]

c. Weekly [ ]

d. Biweekly [ ]

e. Monthly [ ]

f. Rarely [ ]

g. Never [ ]

19. What kind of access do you have on the systems when working remotely?

    a. Weekday working hours (8 am to 5 pm) [ ]

    b. Full time access (24/7) [ ]

    c. Access on request and as required [ ]

20. Do you understand information security policy YES [ ] NO [ ] (tick appropriately)

21. Have you read the information security Policy Document? YES [ ] NO [ ] (tick appropriately)

22. Do you understand the consequences of non-compliance to information security policy? YES [ ]
    NO [ ] (tick appropriately)

**Levels of risk exposure (Environment related)**

23. To what extent do you face power outages while teleworking? Use the scale of 1 to 5 where,

    1-Not at all [ ]

    2-Small extent [ ]

    3-Moderate extent [ ]

    4-Great extent [ ]

    5-Very great extent [ ].

24. Do you have a power backup incase power is interrupted? YES [ ] NO [ ] (tick appropriately)

25. To what extent do you face internet outages while teleworking? Use the scale of 1 to 5 where,

    1-Not at all [ ]

    2-Small extent [ ]

    3-Moderate extent [ ]

    4-Great extent [ ]

    5-Very great extent [ ].

26. Do you have a stable internet backup connection? YES [ ] NO [ ] (tick appropriately)

**For Network and Security Admin Staff only**

27. Are you able to tell who is connected remotely at any one time ? YES [ ] NO [ ] (tick appropriately)
28. Do you give users restricted access to systems? YES [ ] NO[ ] (tick appropriately)
29. Are you able to tell activities being carried out by people connected remotely? YES [ ] NO[ ] (tick appropriately)
30. How often is the Information security policy updated? _____

Thank you for your time