A LINEAR REGRESSION MODEL OF SECURE REMOTE ACCESS TO ENTERPRISE NETWORKS BY EMPLOYEES: A CASE STUDY OF KERICHO COUNTY

BY

KETER KIPKEMOI EDWIN

MASTER OF SCIENCE IN DATA COMMUNICATIONS

KCA UNIVERSITY

2024

A LINEAR REGRESSION MODEL OF SECURE REMOTE ACCESS TO ENTERPRISE NETWORKS BY EMPLOYEES: A CASE STUDY OF KERICHO COUNTY

BY

KETER KIPKEMOI EDWIN

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN DATA COMMUNICATIONS IN THE SCHOOL OF TECHNOLOGY AT KCA UNIVERSITY

SEPTEMBER, 2024

DECLARATION

I declare that the work in this dissertation has not been previously published or submitted elsewhere for award of a degree. I also declare that this my own original work and contains no material written of published by other people except where due reference is made and author duly acknowledged.

Student Name: Keter Kipkemoi Edwin Reg. No: 18/03647

Sign……..…… Date ……20/03/2023…

I do hereby confirm that I have examined this Master Dissertation of

Keter Kipkemoi Edwin

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

Date: 20/03/2026

Dr. Lucy Waruguru Mburu

A LINEAR REGRESSION MODEL OF SECURE REMOTE ACCESS TO ENTERPRISE NETWORKS BY EMPLOYEES: A CASE STUDY OF KERICHO COUNTY

ABSTRACT

The Covid-19 pandemic has made working from home the usual practice for many companies and organizations around the world. While remote work has provided flexibility and kept things running during unusual times, it has also given criminals new chances to take advantage of weaknesses, causing serious cyber-attacks like scams, fake emails, and hacking. Protecting remote work systems is now more important than ever. This study looks at how people working from home handle security problems, develops a special security plan for remote work, and checks if it works well. The study used a survey to gather information about corporate networks and weaknesses in remote access. Data was collected from teleworkers at different levels within organizations to find out what affects remote access security. The process of collecting and analyzing the data was well-organized, and the results were checked using a statistical method called Ordinary Least Squares (OLS) linear regression. This made sure the findings were reliable and accurate.

The research found six important things that affect secure remote access: Technology, Organizational Factors, Employees, Monitoring & Evaluation, Resource Management & Controls, and Data Protection & Monitoring. These six areas together form a guide for companies to improve their information security while allowing employees to work remotely. The OLS linear regression analysis showed that the model can predict remote access security well, with an Adjusted R-squared value of 0.634. This means that the six independent variables explain 63% of the changes in remote access security. ANOVA tests also confirmed that these variables are statistically significant for predicting remote access security.

This research is important for organizations that use county and enterprise networks. The study suggests that organizations should use strong security measures, such as secure devices, employee training, ongoing monitoring, and better management of resources. By following these recommendations, organizations can reduce cybersecurity risks and create safe and efficient remote work settings. This research presents a complete and proven model for teleworking security, designed to handle the special problems caused by working from home during the Covid-19 pandemic. The model provides a useful way for companies to protect their computer networks from increasing cyber dangers. By focusing on safe systems and keeping an eye on potential issues, the study helps improve remote work methods and makes sure companies can stay strong against ongoing cybersecurity problems.

ACKNOWLEDGEMENT

First and foremost, I give thanks to the almighty God for giving me sufficient grace. I extend my appreciation and gratitude to all those that contributed immensely towards completion of this research project.

I am very grateful to my University Supervisor, Dr. Lucy Waruguru Mburu for her tireless assistance, high quality and keenness on details, experience and initiatives, which guided me in enriching and completing this research project.

I owe a debt of gratitude to my family who sacrificed time and gave me invaluable support that saw me through the challenging period. A special thanks to my loving family who were especially supportive in listening to my thoughts and helped me work out logistical details throughout this process.

My gratitude goes to the staff of Kericho County Staff who took their time and effort to provide me with the data necessary to complete this research work. Thank you very much.

To the KCA University school of Technology 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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

ICT- Information and Communication Technology IT- Information Technology

COVID- Corona Virus Disease

Wi-Fi- Wireless Fidelity

MTD - Moving Target Defenses

MFA - Multi-Factor Authentication

APTs - Advanced Persistent Threats

ANN - Artificial Neural Network

ReLu - Rectified Linear Unit

SPSS - Statistical Package for Social Sciences

VPN- Virtual Private Network DT- Deposit Taking

CHAPTER ONE

INTRODUCTION

1.0 The Study's Background

Teleworking is a subset of the broader concept of remote work, having the further distinguishing that technology for communications is used in place of the actual value commute to work (Haber, 2020). This broad notion of telework is described in the literature using a variety of terminology. The problem with existing models for safe remote access to enterprise networks is their inability to properly address the unique security difficulties that enterprises face, particularly in situations such as Kericho County. Many organizations have implemented remote access solutions, but these models may not be suited to the specific demands and circumstances of a specific location or industry. These may include Lack of Customization, Inadequate Threat Intelligence, Compliance and Regulatory Challenges, Limited Scalability, User Experience and Productivity, Integration with Existing Infrastructure, Budgetary Constraints and Local Expertise and Support. Developing a dedicated security model for remote access in the county will address these limitations, providing an effective and tailored solution to safeguard the enterprise networks from potential security threats.

The transition to remote working during the pandemic was accompanied by a sharp spike in cyber-security incidents as thieves tried to profit from the epidemic's stress and disruption as well as the larger "attack surface" they could now target. This has prompted workers and security teams to think about security in a way that was not necessary in the pre-pandemic landscape when work was primarily conducted in a physical workspace. Telecommuting alters the conventional lines between work and non-work globally, which can provide a number of difficulties when crossing numerous temporal, psychological, and

physical borders. The potential for increasing work-life conflict with employees' attempts to maintain a healthy work-life balance is a major obstacle among them.

A significant global economic slowdown has been caused by the most recent, rapid worldwide spread of a novel coronavirus illness (the COVID-19 virus) (Al-Mansour and Al-Ajmi, 2020). Governments imposed a complete state of lockdown, prohibiting all travel and forcing the cessation of all non-essential operations. Many uncomfortable working circumstances were caused by the tight government control procedures. Conventional methods of operation faced significant obstacles. While the 2008 financial crisis had a similar effect on the world economy, COVID-19's long-term effects were more serious. In severely affected regions and industries, such education and healthcare, the effect on firm performance is particularly pronounced. We must implement a temporary COVID-19 strategy with prompt responses from businesses (Ahlstrom and Wang, 2020).

Belzunegui-Eraso and Erro-Garcés estimated that due to the COVID-19 epidemic, approximately 37.6% of employees were engaged in teleworking in May 2020. This figure reflects the substantial shift in work arrangements as a response to the pandemic. One of the notable trends during the pandemic was the significant increase in teleworking across Europe. The proportion of workers in Europe who teleworked at least periodically rose from 11% to 48%. This spike underscores the necessity for remote work arrangements to ensure business continuity and safety during the pandemic. The information hints at the growing prominence of teleworking in lower Africa, which aligns with an emerging body of studies on the subject.

Teleworking has not been confined to developed regions but has found relevance in various parts of the world. The data suggests disparities in teleworking based on demographics. It's noted that even before the outbreak, Black workers were 50% less likely than Europeans and Americans to engage in regular teleworking. This highlights an existing inequality in

remote work opportunities that was further exacerbated by the pandemic. The information reveals fluctuations in teleworking rates over time. Due to COVID-19, teleworking among employed workers surged to 40.6% in 2020 (Belzunegui-Eraso and Erro-Garcés, 2020) However, in subsequent years, these rates decreased, reaching 24.3% in 2021 and 30.9% in 2022. These variations reflect the evolving response to the pandemic and shifting workplace dynamics. The data indicates that in August 2020, Asian workers had a significantly higher rate of teleworking compared to their American, Latino, or African American counterparts. The three-fold difference underscores regional disparities in the adoption of remote work practices. Employees who work remotely or from home can access company servers' hosted data and applications using the internet and similar technologies.

The 1970s oil crisis was initially blamed for the rise in teleworking; thus, it is not an emerging trend. Following the Covid-19 pandemic, it has returned as a precaution to protect employees from contracting Corona virus. The majority of enterprises allowed their workers to work from a location other than the usual office setting, such as their homes (Belal & Rahman, 2021). With the help of numerous internet service providers, people can now purchase laptops and other mobile devices like tablets at reasonable prices, as well as access to reliable power sources.

Even though teleworking has many positive economic and social effects, security is rarely taken into account. While neglecting information security issues, many organizations are happy with how business is done (Sarma, 2022). As the lines between work and home become increasingly porous, wiki-leaks and other sponsored by the state threats, as well as cyberattacks, show the importance of information security in lowering privacy concerns (Belzunegui-Eraso & Erro-Garcés, 2020). Although legally binding control measures like developing an organization's policy on information security possessed a direct effect on cyber security, informal oversight measures like coworkers' influence also had a major effect

regarding data security policy compliance. Concerns about security and privacy are an essential part of cyber-security. The study's empirical findings showed that the employees' safety policy is influenced by both formal and informal controls. However, the authors concluded that employees' compliance is not always a result of the information security policy being implemented (Belzunegui-Eraso & Erro-Garcés, 2020).

A Data Protection Act 2019 was enacted in Kenya in November 2019 as a result of businesses and the government asking citizens to be more vigilant when it comes to data protection. "There are regulations governing the protection of personal data in other nations, such as the General Data Protection Regulation (GDPR) which was established by the European Commission in an effort to bolster and standardize data protection for individuals in the European Union" (Iordache et al., 2021).

1.1 Problem Statement

The proposal's primary concern is on the security issues connected to employees' remote access to corporate networks. Employees' Secure Remote Access to Enterprise Networks Model tries to overcome these pre-existing and heightened security challenges. It underlines the importance of a personalized strategy to remote access security that takes into account the organization's particular requirements, such as Kericho County's, while aligning with best practices and industry standards to protect against growing cybersecurity threats. Organizations can proactively protect their company networks by building a comprehensive model, whether in the context of remote work during COVID-19 or in any other remote work scenario.

Employees need access to organizational assets that transcend the organization's physical borders due to the growing trend of remote work (Belal & Rahman, 2010). However, remote access raises security issues such virus assaults, unauthorized access, and data leaks.

Organization resources in a remote working environment cannot be sufficiently protected by traditional security methods like firewalls and antivirus software. In order to ensure the safety, confidentiality, and accessibility of critical data and resources, a model that offers extensive security protections for the remote access to company networks by employees is required.

Although teleworking carries some risk, it has been less actively handled than other dangers. There are no documented policies, operational processes, or planning in place to warn staff about the dangers of data loss, lower the possibility of hackers, and secure personal information. Teleworking, which enables employees to do their work from any location, is one solution to these problems. However, no regional teleworking security model can effectively execute these working arrangements.

Porcius, 2021 claims that one of the biggest obstacles to the implementation of information security in enterprises is the lack of policies to guide the adoption of solutions. As a result, there have been various efforts over the past several years to create efficient safety standards that are thorough enough to be implemented in the majority of enterprises.

Kericho County's lack of a secure teleworking model can have serious practical consequences for data security, financial stability, public trust, service delivery, and overall efficiency. To prevent these negative consequences, the county must build and implement a strong and specialized secure remote access model that solves the specific security problems and protects its valued resources. Due to these problems, Kericho County put up a working remotely network for its employees. However, due to their lack of routine evaluation and vulnerability to common cyber security threats, the security measures already in place are insufficient (Bett et al., 2022). This project intends to develop a model for safeguarding access to company networks in a teleworking environment, with a focus on remote employees in Kericho County.

The lack of a teleworking model poses a significant challenge in the realm of data communication, particularly in the context of remote access to enterprise networks. Teleworking, or remote work, has become increasingly prevalent in modern workplaces, driven by advancements in technology, changes in work culture, and recent global events such as the COVID-19 pandemic. However, the absence of a well-defined teleworking model can give rise to several data communication problems: Security Risks, Network Performance Issues, Compliance and Regulatory Concerns, Technological Compatibility Challenges, and Employee Training and Support Needs. To address these challenges, organizations must develop and implement a robust teleworking model that encompasses security best practices, performance optimization strategies, compliance frameworks, technological standards, and comprehensive training and support mechanisms.

The choice of using linear regression as the modeling technique in the study of secure remote access to enterprise networks, despite the area being over-studied, can be attributed to several factors: interpretability, assumption of linearity, ease of implementation, baseline comparison, and feature importance make it a valuable tool for gaining insights and informing decision-making in this complex domain.

1.2 The Study's Objectives

1.2.1 General Objective

The proposal's main goal was to establish a linear regression model to predict the safety of remote employee access to corporate networks.

1.2.2 Research Objectives

1. To identify the security dangers connected to employees using remote access to organization networks and the limitations of conventional security procedures in addressing these threats.

2. To investigate the security factors that affect secure remote access by company employees.
3. To develop a linear regression model for remote access to enterprise networks by employees using the identified factors.
4. To test and validate the performance of the developed model.

1.2.2 Research Questions

The study was guided by the following research questions.

1. Which are the security threats that affect remote access to enterprise systems by employees?
2. What measures can be put in place to mitigate the identified security threats?
3. How can regression model can be developed to predict the identified security threats and the corresponding countermeasures?
4. To what extent is the developed model applicable for predicting secure remote access by employees in Kericho County?

1.3 Significance of this Study

The investigation's goal is to identify methods that will guarantee that teleworking, a type of employment that is becoming more and more popular among businesses, is adopted in an appropriate way while limiting the countless possible security exposures associated with it. Organizations and governments are taking action to address cyberthreats as a result of the significant rise in the significance of cybersecurity in recent years across the board of communication and information technology security (Kalakuntla et al., 2019). Teleworking security networks have become increasingly important for maintaining and controlling business operations as a result of Covid-19 regulations that have led to an increase in working remotely.

Regulations that necessitate protected remote utilization of enterprise networks apply to numerous organizations. According to (Kalakuntla et al., 2019), organizations can comply with these rules thanks to the offered model's thorough and efficient solution. Even though telework has been shown to have positive effects on both individuals and society, most organizations have not been enthusiastic about implementing it. This can be because there isn't enough conclusive data to show management whether telework is beneficial to the organizations. In order to answer the question, "Is telework effective for organizations?" this study integrates a regression model to secure remote access to enterprises that reports effects of telework on organizational outcomes.

Many firms have switched to flexible work models as a result of the COVID-19 epidemic, which has expedited the implementation of remote work. The suggested concept enables businesses to give employees protected remote access to corporate networks, allowing them to work remotely while maintaining the protection of corporate assets.

Security architecture (designer) must rise to the challenge of integrating with current security architectures and models across platforms and hosting environments (Kalakuntla et al., 2019). This requires that the architecture be implementation agnostic, extensible, and integrable with current security services. This allows it to be built in terms of any existing security methods, such as Kerberos. Infrastructures for security that are currently in existence cannot be replaced overnight. Similar to this, authentication techniques now in use that are thought to be secure and dependable are kept in use. Each domain normally has its own authorization infrastructure, which is implemented, managed, and supported.

The public sector has frequently lagged other industries in adopting telework, but during the epidemic it has been compelled to do so in order to maintain the delivery of its fundamental functions. The COVID-19 situation has compelled public sector organizations to

use teleworking as their sole choice to carry on with their regular operations and limit the virus' spread (Kalakuntla et al., 2019). It is still too early to fully understand how public employees are responding to the requirements of teleworking, though. We'll do descriptive, correlational, and multiple linear regression analyses. The findings was used to show how teleworking affects factors including productivity, burnout, organizational commitment, and job satisfaction.

The danger of the physical workplace slowly disappearing and, with it, the idea of choice in terms of working remotely should be addressed by policymakers. Employers should make sure that isolation-buffering measures continue as workers in certain segments return to the workplace. The advantages of teleworking are entirely dependent on the level of worker autonomy granted, and they require a culture of trust and compassion, two crucial qualities for leaders to cultivate (Kalakuntla et al., 2019). To prevent a "teleworkability" split, policymakers must address the fundamental issues of ensuring that all employees have access to ICT and have the training and skills necessary to use them.

However, current telework research shows a number of flaws that prevent adoption of this option as a productive means of promoting distributive organizational design. This study was carried out to characterize current telework research, enhance comprehension of telework challenges and issues, and suggest future research possibilities.

1.4 Motivation of the Study

The impetus behind conducting a study on a secure remote access model for enterprise networks by employees is deeply rooted in the evolving landscape of work and the pressing security concerns that have emerged alongside these changes. This study seeks to address the increasing trend of remote work and the associated security risks, which encompass a spectrum of cyber threats, including malware, phishing, password attacks, denial of service attacks, and insider threats. The shift toward remote work arrangements have been gaining momentum,

largely fueled by the convergence of new technologies and the disruptive influence of the COVID-19 pandemic.

Organizations worldwide have been compelled to reevaluate and adapt their operational models. As a result, a substantial number of employees have transitioned to remote work, necessitating their ability to access critical enterprise resources from remote locations, often using their own devices and network connections (Kalakuntla et al., 2019). This transition has brought to the forefront a range of security challenges, threatening the integrity and confidentiality of sensitive corporate data. One of the primary concerns is the heightened risk of unauthorized access to enterprise systems, potentially leading to data breaches and the compromise of proprietary information.

Additionally, the proliferation of remote work has created fertile ground for malicious activities, including malware attacks, phishing attempts, password breaches, and denial of service attacks, which can disrupt essential operations and compromise the security of the entire organization according to (Kalakuntla et al., 2019). The insider threat, another significant security concern, arises from the fact that remote employees have access to sensitive corporate resources. While the majority of remote workers are undoubtedly trustworthy, the potential for internal employees to misuse their privileges and become security threats cannot be overlooked.

In this context, the study aims to develop a robust and comprehensive model for secure remote access to enterprise networks by employees. This model is designed to tackle the intricate and evolving security challenges associated with remote work, ensuring that organizations can effectively safeguard their information and systems (Porcius, 2021). By understanding the unique threats and vulnerabilities linked to remote work, this study seeks to provide practical solutions and insights for businesses and institutions to fortify their security

measures in an era where remote work has become an integral part of the modern work landscape.

Traditional security measures such as firewalls and antivirus software are not sufficient to protect enterprise resources in a remote work environment (Schlehahn, 2020). Therefore, there is a need for a comprehensive and effective security model that addresses the unique security challenges associated with remote access to enterprise networks by employees.

By offering a multi-layered security approach that includes user authentication, access control, data encryption, intrusion detection and prevention, as well as secure communication protocols and VPN technology, the suggested model seeks to close this gap in the literature (Kalakuntla et al., 2019). The goal of the project is to offer employees a secure environment in which they can connect to corporate networks from remote places while maintaining the privacy, accuracy, and accessibility of important information and resources.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

An overview of the literature on secure remote access to enterprise networks by employees is given in the literature study for "A Model of Secure Remote Access to Enterprise Networks by Employees". It draws attention to the many security issues raised by remote access as well as the shortcomings of conventional security methods. Various security mechanisms, such as user authentication, access control, data encryption, and intrusion detection and prevention, can be used to safeguard remote access, and they are all presented in the review.

The rapid adoption of remote working arrangements has transformed organizational operations across the world. Advances in digital technologies have enabled employees to access organizational systems from different locations using remote networks. However, this shift has also introduced significant cybersecurity challenges because remote environments are often less secure than traditional office networks.

Global cyber-security groups and experts have offered guidance and protective techniques to assist people in thwarting fraud and cybercrimes. Because more countries are encouraging their citizens to stay at home, learn, or work from home, putting an emphasis on privacy and security online is more crucial than ever (Seemma et al., 2018). Teleworking encourages a flexible, beneficial relationship between work and family while minimizing the negative effects of movement on the environment. Telework has surprisingly experienced a resurgence in this context due to the measures taken to protect people from the spread of the corona virus (Covid-19). A few governments encouraged teleworking to prevent workers from concentrating on one location in the beginning of 2020.

Using VPN technology, which enables secure connection between remote users and the company network, the assessment highlights VPN technology as a crucial part of remote access security. The evaluation also emphasizes the significance of multi-layered security systems, which combine several security controls to offer complete security (Montagut et al., 2017. The assessment also touches on several earlier investigations that suggested theories for safe remote access to business networks. These studies emphasize the requirement for all-encompassing security measures, which should include user authentication, access control, data encryption, and intrusion detection and prevention.

This dissertation presents an explanation of cyber-attacks that offers the terminology and concepts necessary to fully assess the efficacy of MTD systems. Some claim that Moving Target Defenses (MTD) will completely transform computer security by eliminating the staleness of current computer systems. Although MTD systems seem promising, it is difficult to understand and foresee how they will affect protection, subscribers, and hackers (Montagut et al., 2017). Although an explanation of MTD systems has been proposed, there is yet no established model of cyber-attacks that can be used to comprehend and analyze how hackers and MTD systems interact.

2.1 Theoretical Framework

The proposed theoretical framework constitutes a comprehensive and layered approach to information security, intending to safeguard remote access to corporate enterprise networks. It incorporates a multi-layered security strategy encompassing user identification, access control, data encryption, intrusion detection and prevention, as well as secure communication protocols (Porcius, 2021). This strategic approach is rooted in the principle of "defense in depth," a concept widely recognized in the field of information security.

This concept underpins the methodology, advocating for the integration of multiple layers of security measures to create a robust defense system against a wide array of security risks. The fundamental premise is that no single security measure is sufficient to ensure comprehensive protection according to (Porcius, 2021). Instead, by employing multiple layers of defense, an organization can significantly enhance its resilience and ability to thwart security threats. Each layer is designed to counter specific types of threats, thus providing a comprehensive security net.

The proposed model also embraces the principle of least privilege, a foundational concept in information security. This principle dictates that access to sensitive information and resources should be restricted to only authorized users and processes (Seemma et al., 2018). By adhering to this principle, the model minimizes the risk of unauthorized access and potential data breaches.

To bolster the security infrastructure, the framework integrates established security protocols and technologies. One notable inclusion is Virtual Private Network (VPN) technology. VPNs are instrumental in ensuring secure remote connections by encrypting data transmissions and establishing secure tunnels between remote users and the organization's network (Porcius, 2021). The use of VPN technology is a pivotal step in guaranteeing data privacy and security during remote access.

Recognizing the importance of user identification and authentication, the model incorporates robust authentication techniques, with a specific focus on multi-factor authentication (MFA). According to (Seemma et al., 2018). MFA is an advanced authentication method that requires users to provide multiple forms of verification to confirm their identity. This approach adds an extra layer of security, making it significantly more challenging for unauthorized users to gain access.

The proposed framework introduces the concept of dividing the company network into distinct zones, each with varying levels of security requirements. These zones are demarcated based on the roles and responsibilities of remote users. Access to network resources is governed by the access control regulations established within the model. These regulations dictate which resources and zones a user or process can access, aligning with their authorized privileges.

The theoretical framework offers a comprehensive and structured approach to secure remote access. It acknowledges the complexity of modern security challenges and strives to address them by adopting a multi-layered defense system (Porcius, 2021). By adhering to principles like defense in depth and the least privilege concept, the model ensures that remote access remains secure and protected against a broad spectrum of security threats. The integration of well-established security protocols and technologies, alongside robust authentication techniques, further fortifies the security posture (Seemma et al., 2018). Additionally, zoning the network provides an organized and controlled environment, where access control is customized to match the roles and responsibilities of remote users (Porcius, 2021). Overall, the proposed framework is designed to provide a comprehensive and robust defense against the evolving landscape of security risks in remote corporate network access.

2.1.1 MTD System Theory

In an era where cyber threats are evolving at an alarming pace and attackers continuously seek innovative ways to compromise networks and systems, traditional static cybersecurity measures are proving insufficient in safeguarding sensitive data and maintaining the integrity of enterprise networks (Bagaskara et. al., 2021). Moving Target Defense (MTD) is an emerging and adaptive cybersecurity approach that aims to counteract this ever-evolving threat landscape. MTD seeks to transform the traditional security paradigm by introducing dynamic, agile, and adaptable strategies designed to thwart potential adversaries. In this

discussion, we will delve into the MTD system theory and explore its relevance to Secure Remote Access to Enterprise Networks by Employees.

According to (Bagaskara et. al., 2021) MTD is grounded in the concept of moving or constantly altering the target that attackers must breach to compromise a system or network. The core idea is to create an environment where potential adversaries face a shifting, hostile, and unpredictable landscape, making it exceedingly challenging for them to identify and exploit vulnerabilities. This approach fundamentally challenges traditional static security measures and introduces a set of principles and strategies designed to adapt to the dynamic nature of modern cyber threats.

MTD promotes the frequent and unpredictable alteration of network configurations. This involves changing IP addresses, ports, server locations, and other network attributes. The objective is to create a constantly shifting landscape for potential attackers, thereby minimizing their ability to target specific vulnerabilities (Bagaskara et. al., 2021).

Deception is a cornerstone of MTD. It entails the creation of decoy systems, services, and data to divert and confuse attackers. By introducing fake targets alongside legitimate assets, organizations can increase the attacker's uncertainty and reduce the likelihood of a successful breach as illustrated by (Bagaskara et. al., 2021).

MTD encourages the use of evasive technologies that allow organizations to hide their true assets and configurations. Techniques may include network cloaking, which conceals network topologies, and application layer diversification, which disguises application behaviors (Bagaskara et. al., 2021).

MTD emphasizes the importance of real-time monitoring and analysis of network traffic and system behaviors. Continuous assessment of network activity enables the timely detection of suspicious patterns or anomalies that may indicate an ongoing attack.

An essential element of MTD is the ability to respond rapidly and adapt to detected threats. When potential security breaches are identified, automated responses can be triggered to counteract the attack, isolate compromised systems, and initiate incident response procedures (Bagaskara et. al., 2021).

The relevance of the MTD system theory to the case study of Model of Secure Remote Access to Enterprise Networks by Employees: A Case Study of Kericho County is apparent in several key aspects:

Implementing a dynamic network configuration within the Kericho County's remote access security model can enhance defense against external threats. According to (Bagaskara et. al., 2021), by regularly changing network parameters and configurations, the model can thwart attackers who rely on static reconnaissance for vulnerabilities.

The integration of deception mechanisms can be particularly valuable in the case study. By introducing deceptive assets or information within the network, attackers are led astray, making it challenging for them to pinpoint genuine resources. This adds an extra layer of security to the remote access environment (Bagaskara et. al., 2021).

Leveraging evasive technologies within the security model can help hide critical network assets and configurations. By cloaking network topologies and diversifying application behaviors, the system becomes less predictable for potential attackers.

Real-time monitoring and analysis are essential components of a secure remote access model. By continuously assessing network traffic and system behaviors, any unusual or suspicious activities can be promptly identified, triggering a rapid response to potential security threats (Bagaskara et. al., 2021).

In the event of a detected threat or breach, an adaptive response mechanism becomes critical. Automated responses can be employed to mitigate the impact of the attack, isolate

compromised systems, and initiate incident response procedures, ultimately reducing the potential damage and exposure of sensitive data.

The integration of MTD principles and strategies into the Kericho County's security model can significantly enhance its effectiveness in securing remote access to enterprise networks, particularly in the face of evolving and persistent cyber threats (Bagaskara et. al., 2021).

Moving Target Defense (MTD) represents a paradigm shift in cybersecurity, advocating for dynamic and adaptive strategies to counteract the continually evolving cyber threat landscape. The relevance of MTD to the case study of Kericho County's remote access security model is evident in its potential to enhance the model's resilience and effectiveness. By embracing the principles of MTD, organizations can significantly bolster their security posture, making it more adaptable and robust against a broad spectrum of security threats (Bagaskara et. al., 2021). In a digital landscape where traditional security measures are often insufficient, MTD offers a promising path forward for organizations seeking to secure their remote access environments effectively.

2.1.2 The Theory of Cyber Attack

The theory provides a framework for comprehending the many phases of a cyber-attack and the driving forces behind it, which can guide the development and application of security measures in the model. Information about the target system and identifying vulnerabilities are part of the reconnaissance phase of a cyber-attack (Bada, Sasse & Nurse, 2019). An attacker may try to find holes in the security measures or network configurations that the remote access system is using in the context of remote access to enterprise networks. Since employees shouldn't unintentionally expose sensitive information, the model should also incorporate user

education and training programs to avoid such reconnaissance attempts from being detected and prevented (Bada, Sasse& Nurse, 2019).

The exploitation stage of a cyber-attack involves using the gathered information to exploit vulnerabilities in the target system. In the context of remote access to enterprise networks, this may involve exploiting weaknesses in the authentication or access control mechanisms used by the remote access system (Clakre, 2021). To prevent this, the model should include strong authentication mechanisms and access controls, such as multi-factor authentication and role-based access control, to prevent unauthorized access.

According to (Janczewski & Colarik, 2021), the infiltration stage of a cyber-attack involves retrieving and extracting the desired data or resources from the target system. In the context of remote access to enterprise networks, this may involve stealing sensitive data or information from the network. To prevent this, the model should include data encryption and data loss prevention mechanisms to protect sensitive information from unauthorized access or disclosure.

In the context of the case study in Kericho County, the theory of cyber-attacks holds significant relevance. As organizations, including public entities like county governments, increasingly adopt remote work models, the attack surface expands (Janczewski & Colarik, 2021). Cyber attackers are well aware of this trend and are continually developing more sophisticated techniques to exploit vulnerabilities. Here's how the theory of cyber-attacks relates to the case study:

Vulnerability Identification: Cyber attackers seek to identify vulnerabilities in remote access systems, including flaws in network configurations, outdated software, or weaknesses in authentication mechanisms. The secure remote access model must consider these vulnerabilities and employ strategies to mitigate them effectively (Clakre, 2021).

Social Engineering: Given that many remote workers use personal devices, social engineering attacks, such as phishing, can target employees working from home. The model must include robust training and awareness programs to educate employees about these threats and how to recognize them (Kim & Solomon, 2018).

Insider Threats: Remote workers, while trusted employees, can pose insider threats if their devices are compromised or if they accidentally expose sensitive information. The model should include controls and monitoring mechanisms to detect and mitigate insider threats (Kim & Solomon, 2018).

Advanced Persistent Threats (APTs): Organizations like county governments may be attractive targets for APTs seeking to gain unauthorized access to sensitive information (Clakre, 2021). The model must incorporate advanced threat detection and response mechanisms to counter such threats effectively.

Zero-Day Exploits: As attackers continually search for unknown vulnerabilities, the model must include rapid patching and updating of software and systems to reduce the exposure to zero-day exploits (Kim & Solomon, 2018).

Ransomware and Malware: According to (Whitman & Mattord, 2018) remote workers' devices can become entry points for ransomware and malware attacks. Robust endpoint security measures, including anti-malware software and regular backups, are crucial components of the model.

Secure Communication: Cyber-attacks can target data in transit, emphasizing the importance of secure communication protocols, such as VPN technology, in the model (Janczewski & Colarik, 2021).

According to (Clakre, 2021), understanding the theory of cyber-attacks is fundamental to designing an effective secure remote access model. In the case of Kericho County, where

remote work is becoming increasingly prevalent, the implications of cyber-attacks are substantial. By considering the full spectrum of potential threats, including vulnerabilities, social engineering, insider threats, APTs, and emerging attack techniques, the model can be tailored to provide robust security measures and safeguard sensitive information effectively (Whitman & Mattord, 2018).

2.2 Factors Affecting Cybersecurity

Cybersecurity in organizations is influenced by several technological, organizational, and human factors. As institutions increasingly adopt remote working systems, protecting organizational information has become more complex. Employees working outside the traditional office environment often access organizational systems using personal devices, home networks, or public internet connections. These environments may not have the same level of protection that exists within secured organizational networks. As a result, organizations must implement effective cybersecurity measures to ensure the confidentiality, integrity, and availability of their information systems. Several key factors influence the effectiveness of cybersecurity in remote working environments, including remote work security practices, cybersecurity threats in teleworking environments, virtual private network (VPN) security, multi-factor authentication, and insider threats.

In accordance with (Zeng & Li, 2020), cyber security has grown significantly in the realm of information technology since information security is now a major concern for every business and government in the globe. Governments as well as organizations are taking certain actions to counteract cyber risks since they can cause damages that range from interpersonal criminal activity to the blackmail of large companies and nations (Kalakuntla et al., 2019). Cyber-security is crucial in the realm of data technology given that protecting information is a growing concern for businesses and governments today (Porcius, 2021). Cyber-security is impacted by a number of issues, some of which are listed here.

Human error remains one of the most significant factors affecting cybersecurity. Employees can inadvertently compromise security through actions like clicking on malicious links, falling victim to phishing attacks, or mishandling sensitive data. With remote employees using personal devices, the risk of human error increases. Training and awareness programs are crucial to educate employees about the risks and best practices associated with remote work.

Lack of cyber-security awareness: Many security breaches occur due to a lack of security awareness among employees (Porcius, 2021). Training and education are crucial in preventing common security lapses. To address this factor, the model should prioritize ongoing security awareness programs that are accessible to remote employees.

Software vulnerabilities: Outdated software, unpatched systems, and vulnerable hardware create opportunities for cyber attackers to exploit weaknesses in the technology stack. Zero-day vulnerabilities, in particular, pose significant risks (Porcius, 2021). The model must ensure that all systems used for remote access are regularly updated and patched to mitigate technology vulnerabilities. The use of secure communication protocols, like VPN technology, is vital in this context.

Insider threats: Malicious or negligent insiders, including employees, contractors, or business partners, can pose significant risks to cybersecurity by intentionally or unintentionally compromising data security. The model must include controls to monitor and detect insider threats among remote employees, as these individuals can inadvertently compromise data security.

Cyber-criminal activity: Cybercriminals often use social engineering techniques to manipulate individuals into revealing sensitive information or performing actions that compromise security. This includes tactics like phishing, pretexting, baiting, and tailgating. Remote workers can be targeted by social engineering attacks, such as phishing (Kalakuntla et

al., 2019). The model should include mechanisms to detect and prevent these attacks, coupled with robust employee training to recognize and report suspicious activity.

Lack of security protocols: Many security breaches occur due to a lack of security awareness among employees (Kalakuntla et al., 2019). Training and education are crucial in preventing common security lapses. To address this factor, the model should prioritize ongoing security awareness programs that are accessible to remote employees.

Third-party risks: Organizations often rely on third-party vendors, which can introduce security risks if not properly vetted. The security practices of third parties should align with the organization's security standards (Porcius, 2021). Any third-party tools or services used in the remote access model should be thoroughly vetted for security and compliance with data protection regulations.

Malware and Ransomware: The proliferation of malware and ransomware poses a severe threat. These malicious software types can infiltrate systems, encrypt data, and demand ransoms for decryption keys (Porcius, 2021). Malware and ransomware can infiltrate remote workers' devices. Endpoint security, including anti-malware software, should be a fundamental component of the model.

Regulatory Compliance: Compliance with data protection and privacy regulations is essential. Failing to meet these standards can lead to legal consequences and breaches of sensitive data. Compliance with data protection regulations should be a core aspect of the model, ensuring that remote access aligns with legal requirements.

Remote Work Environments: According to (Kalakuntla et al., 2019), the rapid increase in remote work introduces new challenges to cybersecurity. Remote employees accessing corporate networks from various locations can be targeted by cybercriminals. The

entire model is focused on securing remote access to enterprise networks, making it crucial for mitigating the risks introduced by remote work environments.

Factors affecting cybersecurity have a direct impact on the design and implementation of secure remote access models. In the Kericho County case study, the relevance of these factors is evident, as the county government adapts to a remote work model. To ensure the security of enterprise networks in this changing landscape, the model should incorporate strategies and measures that address these factors effectively.

2.2.1 Remote Work Security

Remote work security refers to the measures that organizations put in place to protect information systems when employees access organizational resources from outside the workplace. With the rapid adoption of teleworking, many organizations have had to adjust their cybersecurity strategies to accommodate employees working from different locations. While remote work offers flexibility and increased productivity, it also introduces new risks to organizational systems.

Employees working remotely often rely on home networks, which may not have strong security configurations. For example, home Wi-Fi networks may use weak passwords or outdated encryption protocols, making them vulnerable to cyberattacks. In addition, employees may use personal computers or mobile devices that lack proper security updates or antivirus software. These vulnerabilities can create entry points for attackers who may attempt to access sensitive organizational data.

To reduce these risks, organizations must implement clear remote work security policies and ensure that employees understand how to protect organizational information when working remotely. Training employees on cybersecurity awareness is also important because

many security breaches occur due to human error. By educating employees about safe online practices, organizations can significantly reduce the likelihood of cyber incidents.

2.2.2 Cybersecurity Threats in Teleworking

Teleworking environments expose organizations to a wide range of cybersecurity threats. When employees work remotely, organizational networks extend beyond the physical office environment, which increases the potential attack surface for cybercriminals. Some of the most common threats associated with teleworking include phishing attacks, malware infections, ransomware attacks, and unauthorized access to organizational systems.

Phishing attacks are among the most common cyber threats affecting remote workers. In such attacks, cybercriminals send fraudulent emails or messages designed to trick employees into revealing sensitive information such as login credentials or financial data. Because remote employees rely heavily on email communication, they may be more vulnerable to such attacks if they are not properly trained to identify suspicious messages.

Malware and ransomware attacks also pose serious risks to organizations. Malware refers to malicious software that can damage systems, steal data, or disrupt operations. Ransomware is a type of malware that encrypts files and demands payment before the data can be restored. These attacks can have severe financial and operational consequences for organizations, especially when critical data becomes inaccessible.

Organizations must therefore implement strong cybersecurity monitoring systems, conduct regular security assessments, and educate employees on recognizing potential threats. By taking proactive measures, organizations can reduce the risks associated with teleworking environments.

2.2.3 Virtual Private Network (VPN) Security

A Virtual Private Network (VPN) is an important tool used by organizations to secure remote connections to internal systems. A VPN creates a secure and encrypted communication channel between a remote user and the organization's network. This encryption ensures that data transmitted over the internet cannot easily be intercepted by unauthorized individuals.

When employees connect to organizational systems through a VPN, their internet traffic is protected, which reduces the risk of data interception or unauthorized access. VPNs are particularly important for employees who access organizational resources from public networks such as hotels, airports, or coffee shops, where cyber threats are more common.

However, the effectiveness of VPN security depends on proper implementation and usage. Organizations must ensure that VPN systems are regularly updated and monitored to detect unusual activity. Employees should also be required to use VPN connections whenever they access organizational systems remotely. By enforcing VPN usage policies, organizations can significantly improve the security of remote network connections.

2.2.4 Multi-Factor Authentication

Multi-factor authentication (MFA) is another important cybersecurity measure used to protect organizational systems. MFA requires users to provide more than one form of identification before gaining access to a system. Instead of relying solely on a password, users may also need to verify their identity through additional methods such as a one-time code sent to their mobile phone, a fingerprint scan, or a security token.

Passwords alone are often not sufficient to protect sensitive systems because they can be easily guessed, stolen, or compromised through phishing attacks. By adding additional

layers of authentication, MFA makes it much more difficult for attackers to gain unauthorized access to organizational systems.

Many organizations have adopted MFA as part of their cybersecurity strategies, especially for remote access systems. This approach helps ensure that even if login credentials are compromised, unauthorized users cannot easily access organizational resources. As remote work becomes more common, MFA will continue to play a critical role in strengthening cybersecurity defenses.

2.2.5 Insider Threats in Remote Networks

Insider threats represent another significant challenge for organizational cybersecurity. Unlike external cyberattacks, insider threats originate from individuals within the organization, such as employees, contractors, or partners who have legitimate access to organizational systems. These threats can occur intentionally or unintentionally.

Intentional insider threats may involve employees deliberately stealing sensitive information for personal gain or sharing confidential data with unauthorized individuals. Unintentional insider threats, on the other hand, occur when employees unknowingly compromise security through careless actions. For example, an employee might accidentally send confidential information to the wrong recipient or store sensitive files on unsecured devices.

Remote work environments can increase the risk of insider threats because employees operate outside the direct supervision of organizational IT departments. Organizations must therefore implement strong access control policies, monitor system activities, and ensure that employees understand their responsibilities in protecting organizational data.

Regular cybersecurity training and clear organizational policies can help reduce the risk of insider threats. By promoting a culture of cybersecurity awareness, organizations can encourage employees to take an active role in protecting organizational information systems.

2.3 Conceptual Framework

A conceptual framework provides a structured way of understanding the relationship between different variables in a study. It helps explain how certain factors influence a particular outcome. In this research, the conceptual framework illustrates how different organizational, technological, and human factors influence cybersecurity in remote access systems. The framework identifies the key independent variables that affect the level of cybersecurity within organizations that implement remote working arrangements.

As organizations adopt teleworking systems, employees are able to access organizational resources from locations outside the traditional office environment. While this approach increases flexibility and productivity, it also introduces cybersecurity risks. The conceptual framework in this study therefore focuses on identifying the key factors that influence the effectiveness of cybersecurity measures when employees access organizational systems remotely.

The dependent variable in this study is cybersecurity in remote access environments, while the independent variables include technological factors, organizational factors, environmental factors, employee awareness, and security policies. These variables interact in different ways to determine how well an organization can protect its information systems and data when remote access technologies are used.

2.3.1 Technological Factors

Technological factors play a critical role in determining the level of cybersecurity within an organization. These factors refer to the tools, systems, and technologies used to protect organizational networks and data from cyber threats. When employees access systems remotely, strong technological security measures are required to ensure that sensitive information is protected from unauthorized access.

Examples of technological security measures include firewalls, intrusion detection systems, virtual private networks (VPNs), encryption technologies, and secure authentication mechanisms. These tools help protect data as it travels between remote devices and organizational servers. For instance, VPN technology encrypts internet traffic, ensuring that confidential information cannot easily be intercepted by cybercriminals.

Organizations that invest in modern cybersecurity technologies are generally better prepared to protect their systems against cyber threats. However, technology alone is not sufficient if it is not properly configured and managed. Regular system updates, security monitoring, and vulnerability assessments are essential for maintaining strong technological defenses. Therefore, technological factors significantly influence the effectiveness of cybersecurity in remote working environments.

2.3.2 Organizational Factors

Organizational factors refer to the internal structures, policies, and management practices that guide how cybersecurity is implemented within an organization. Strong organizational support is necessary to ensure that cybersecurity strategies are effectively developed and enforced.

One important organizational factor is the availability of clear cybersecurity policies that define how employees should handle organizational data and systems. These policies

provide guidelines on password management, secure communication, remote access procedures, and data protection practices. When employees understand these policies, they are more likely to follow secure practices while performing their duties.

Another important organizational factor is management commitment to cybersecurity. Organizational leaders play a crucial role in allocating resources for cybersecurity initiatives, including training programs, security tools, and monitoring systems. Without adequate support from management, cybersecurity measures may not be effectively implemented or maintained.

In addition, organizations must establish strong IT governance structures to monitor compliance with cybersecurity policies. Regular audits, system monitoring, and incident response procedures help ensure that potential security threats are detected and addressed in a timely manner. Therefore, organizational factors are essential in strengthening the overall cybersecurity posture of institutions that rely on remote access technologies.

2.3.2 Environmental Factors

Environmental factors refer to external conditions that influence cybersecurity practices within organizations. These factors may include technological developments, regulatory requirements, and the broader cybersecurity landscape in which an organization operates.

For example, the increasing sophistication of cyber threats requires organizations to continuously improve their cybersecurity strategies. Cybercriminals constantly develop new attack methods such as ransomware, phishing schemes, and advanced malware. As a result, organizations must remain vigilant and adopt proactive measures to protect their systems.

Government regulations and data protection laws also influence how organizations manage cybersecurity. Many countries have introduced regulations that require organizations

to implement specific security measures to protect sensitive data. Compliance with such regulations encourages organizations to strengthen their cybersecurity practices.

In addition, environmental factors such as internet infrastructure and access to digital technologies can influence the effectiveness of remote work systems. Organizations operating in environments with limited technological infrastructure may face additional challenges when implementing secure remote access solutions. Therefore, environmental factors can significantly shape the cybersecurity strategies adopted by organizations.

2.3.3 Employee Awareness

Employee awareness is another important factor that influences cybersecurity within organizations. Employees are often considered the first line of defense against cyber threats because they interact directly with organizational systems and data on a daily basis. However, human error remains one of the most common causes of cybersecurity incidents.

Many cyberattacks exploit human weaknesses rather than technological vulnerabilities. For example, phishing attacks attempt to trick employees into revealing confidential information such as login credentials or financial details. If employees are not aware of such threats, they may unknowingly compromise organizational systems.

To address this challenge, organizations must invest in cybersecurity awareness training programs. These programs educate employees about common cyber threats and teach them how to recognize suspicious activities. Training may include guidance on identifying phishing emails, creating strong passwords, and safely handling sensitive information.

Continuous awareness programs help create a culture of cybersecurity within organizations. When employees understand the importance of protecting organizational data,

they are more likely to follow secure practices while working remotely. As a result, employee awareness significantly contributes to strengthening cybersecurity in remote access environments.

2.3.4 Security Policies

Security policies provide the formal guidelines that regulate how organizational information systems should be used and protected. These policies outline acceptable behaviors for employees and establish procedures for managing cybersecurity risks.

Effective security policies typically cover areas such as password management, data protection, remote access procedures, system monitoring, and incident response. These guidelines help ensure that all employees follow consistent security practices when accessing organizational systems.

In remote working environments, security policies are particularly important because employees operate outside the traditional office environment. Clear policies ensure that employees understand the rules governing remote access and the steps they must take to protect organizational data.

Organizations must also ensure that security policies are regularly updated to address emerging cyber threats and technological changes. In addition, employees should be trained on how to apply these policies in their daily work activities. By enforcing strong security policies, organizations can reduce vulnerabilities and improve their ability to protect sensitive information.

2.3.5 Relationship Between the Variables

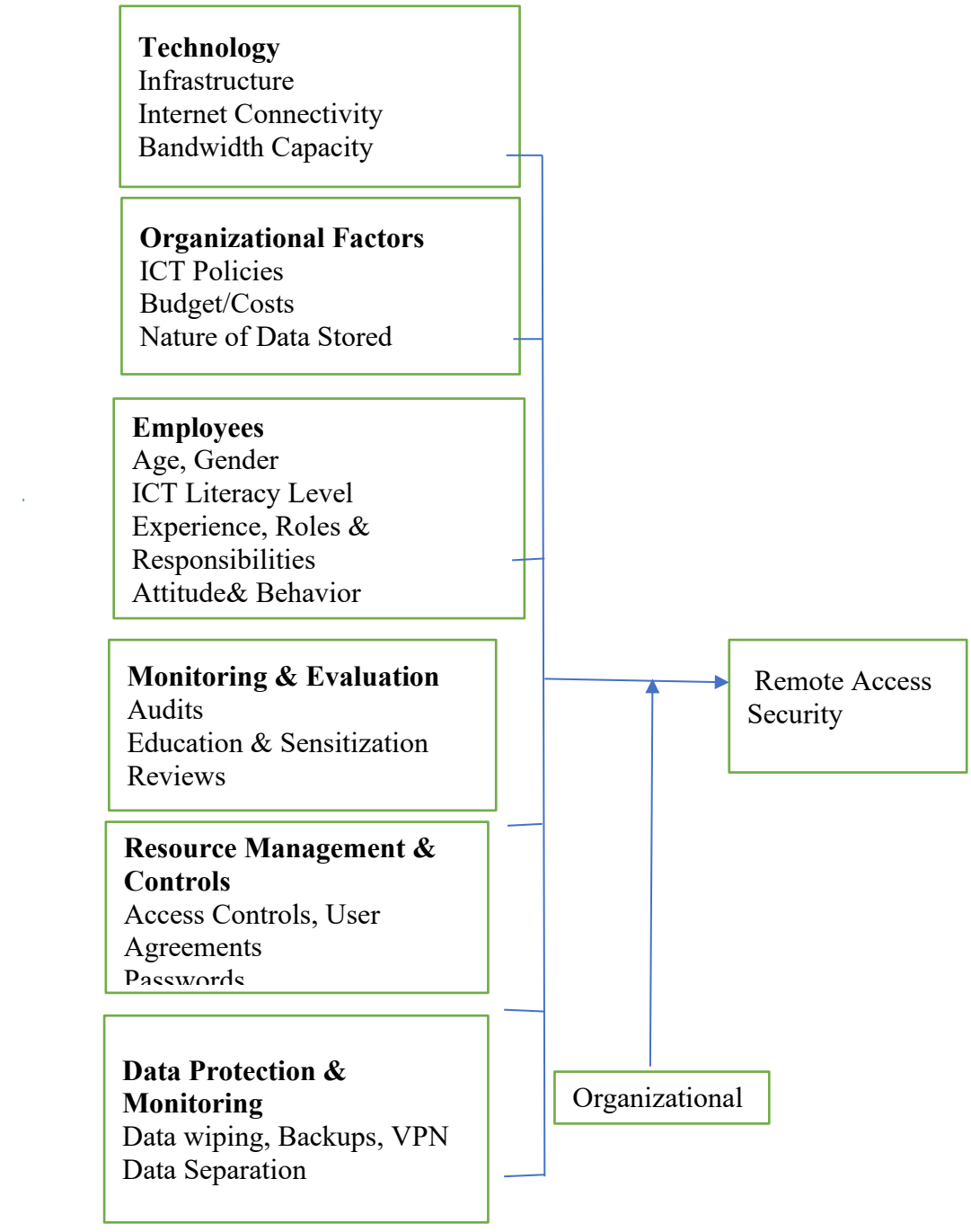
The variables presented in the conceptual framework are interconnected and collectively influence cybersecurity outcomes in organizations. Technological factors provide the tools and systems required to protect networks and data. Organizational factors ensure that proper management structures and policies are in place to support cybersecurity initiatives. Environmental factors shape the external conditions under which organizations operate, including regulatory requirements and evolving cyber threats.

At the same time, employee awareness ensures that individuals understand their role in protecting organizational systems. Even the most advanced cybersecurity technologies can fail if employees do not follow secure practices. Security policies provide the guidelines that integrate these different elements and ensure consistent implementation of cybersecurity measures.

Together, these variables influence the overall effectiveness of cybersecurity strategies in organizations that rely on remote access technologies. By understanding the relationship between these factors, organizations can develop comprehensive cybersecurity frameworks that address both technical and human vulnerabilities.

FIGURE 2.1

The Conceptual Framework of the Proposed Model



2.3.2 Operationalization of variables

In the context of this research study, the selection and definition of variables are of utmost importance. These variables serve as the building blocks of the study, allowing

researchers to quantify, measure, and analyze the phenomena of interest (Bourne, 2022). In this discussion, we delved into the significance of defining variables in a measurable form and how these variables were summarized through indicators and values. We also explored the specific example provided in the context of the study, where the dependent variable, remote access security, defined as a binary number. Measurable variables allow for consistency in data collection and analysis. When variables are clearly defined, it reduces ambiguity and ensures that different researchers or research teams can replicate the study's methods and obtain similar results. Measurable variables enable meaningful comparisons (Bourne, 2022). Researchers can compare data across different groups, time periods, or conditions, providing insights into patterns, trends, and differences.

Numerical variables can be subjected to a wide range of statistical analyses, from descriptive statistics like means and standard deviations to more complex techniques such as regression analysis and data mining. These analyses help uncover relationships and associations within the data. Indicators are specific measurements or attributes that capture the essence of a variable. They serve as operational definitions of the variable, allowing researchers to collect and quantify data related to that variable. For instance, if the variable of interest is "employee satisfaction," indicators may include factors like job satisfaction, work-life balance, or compensation.

The dependent variable, Remote access security, was defined as a binary number with two possible values: 0 and 1. In this context, a binary variable is used to represent a dichotomous outcome, where 0 denotes the absence of an effect or efficacy, and 1 denotes the presence of an effect or efficacy. This binary approach simplifies the outcome into two distinct categories, making it suitable for certain types of analysis, such as logistic regression.

In the study, the binary variable was likely used to assess whether teleworking has a positive effect (1) or no significant effect (0) on a particular outcome or dependent variable. This simplification can be useful when studying complex phenomena, as it provides a clear and interpretable outcome.

Defining variables in a measurable form with clear indicators and values is a fundamental aspect of research. It enables researchers to collect, analyze, and interpret data effectively. In the case of the study, the binary dependent variable adds a layer of simplicity to the analysis, making it easier to draw conclusions about the efficacy of teleworking. In the context of the study, Table 2.1 summarizes the indicators and values for each variable. Each indicator has a corresponding numerical value that quantifies its presence or degree. These values are derived from the count of unique entries identified in the database, indicating the frequency or prevalence of each indicator within the dataset.

TABLE 2.1

Operationalization of Variable

Variables	Indicator
Remote Access System	Type of remote access technology: This variable refers to the type of technology used by employees to remotely access the enterprise network. For example, the remote access system could use VPN, cloud-based remote desktops, or remote desktop protocol (RDP) software. The operationalization of this variable could involve measuring the number of employees using each type of technology. Number of users accessing the remote access system: This variable measures the number of employees who access the remote access system. This could be operationalized by tracking the number of active user accounts on the remote access system. Level of encryption used for data transmitted through the remote access system: This variable measures the strength of the encryption used to protect data transmitted between the remote access system and the enterprise network. The operationalization of this variable could involve measuring the level of encryption (e.g., 128-bit or 256-bit) used by the remote access system.

Employee Behavior	Frequency of password changes: This variable measures the frequency with which employees change their remote access passwords. The operationalization of this variable could involve tracking the number of password changes made by employees over a given period (e.g., month or quarter). Percentage of employees who complete cybersecurity training: This variable measures the proportion of employees who have completed cybersecurity training. The operationalization of this variable could involve calculating the percentage of employees who have completed a cybersecurity training program. Rate of employees who report suspicious emails or activity: This variable measures the rate at which employees report suspicious emails or activity related to the remote access system. The operationalization of this variable could involve tracking the number of reports of suspicious activity made by employees over a given period.
Cyber-security Policies	Number of access control policies in place: This variable measures the number of access control policies implemented by the enterprise to protect the remote access system. The operationalization of this variable could involve counting the number of access control policies (e.g., password policies, multi-factor authentication requirements) in place. Frequency of security policy review and update: This variable measures how often security policies are reviewed and updated. The operationalization of this variable could involve tracking the frequency with which security policies are reviewed and updated (e.g., monthly, quarterly, annually). Percentage of employees who have read and signed off on the security policies: This variable measures the proportion of employees who have read and agreed to the enterprise's security policies. The operationalization of this variable could involve calculating the percentage of employees who have read and signed off on the security policies.
Threats and Vulnerabilities	Number of successful phishing attacks on employees accessing the remote access system: This variable measures the number of successful phishing attacks carried out against employees who use the remote access system. The operationalization of this variable could involve counting the number of successful phishing attacks over a given period. Frequency of malware detection on devices accessing the remote access system: This variable measures how often malware is detected on devices that access the remote access system. The operationalization of this variable could involve tracking the number of malware detections on remote access devices over a given period.

	Number of incidents of unauthorized access to the remote access system: This variable measures the number of incidents of unauthorized access to the remote access system. The operationalization of this variable could involve tracking the number of incidents of unauthorized access to the remote access system over a given period.
Security Measures	Number of devices with two-factor authentication enabled: This variable measures the number of remote access devices that have two-factor authentication enabled. The operationalization of this variable could involve counting the number of remote access devices that have two-factor authentication

Defining variables in a measurable form with clear indicators and values is a fundamental aspect of research. It enables researchers to collect, analyze, and interpret data effectively. In the case of the study, the binary dependent variable adds a layer of simplicity to the analysis, making it easier to draw conclusions about the efficacy of teleworking. In the context of the study, Table 2.1 summarizes the indicators and values for each variable. Each indicator has a corresponding numerical value that quantifies its presence or degree. These values are derived from the count of unique entries identified in the database, indicating the frequency or prevalence of each indicator within the dataset.

2.4 Research Gap

In the evolving landscape of cybersecurity, the significance of addressing insider threats within the framework of secure remote access to corporate networks has become increasingly apparent. While conventional security measures such as authentication, encryption, and access controls are effective in thwarting external threats, the challenge lies in identifying and preventing risks posed by authorized users who possess legitimate network access (Sarma, 2022). This discussion delves into the concept of insider threats and explores potential research gaps in creating more robust techniques for identifying and mitigating these threats within secure remote access models.

Insider threats, a significant concern in the realm of cybersecurity, refer to the risks posed by individuals within an organization who have authorized access to the network and exploit their privileges for malicious purposes. These threats may manifest as data theft, data destruction, or other forms of unauthorized activity, often with potentially devastating consequences. The unique nature of insider threats lies in the fact that these individuals are already within the organization's trusted perimeter, making them harder to detect and mitigate.

As organizations increasingly adopt remote work models, the potential for insider threats escalates, necessitating the development of more sophisticated techniques to detect and mitigate such risks (Sarma, 2022). One notable research gap within the domain of secure remote access models pertains to the creation of enhanced methods for identifying and blocking insider threats.

Complexity of Insider Threat Detection: Identifying insider threats is a multifaceted challenge. While external threats often exhibit distinct patterns, insider threats may be subtler and difficult to discern. Traditional security measures may not suffice to detect these threats effectively.

Dynamic Nature of User Behavior: Insider threats may involve personnel who have legitimate access to the network and, as a result, exhibit typical user behavior. It is critical to develop methodologies capable of distinguishing between legitimate and suspicious user activities.

The Need for Real-Time Monitoring: To effectively thwart insider threats, organizations need real-time monitoring and analysis capabilities. This entails the continuous evaluation of user behavior and the prompt identification of potential threats (Sarma, 2022). To bridge this research gap and fortify secure remote access models, several potential research directions can be explored.

Behavioral Analysis Using AI and Machine Learning: Leveraging artificial intelligence (AI) and machine learning technologies can aid in the analysis of user behavior to identify anomalies and potential threats. By establishing baseline behavior patterns, deviations can be swiftly identified and investigated.

Research may investigate behaviorally based access controls that adapt access privileges in response to user activity. Rather than relying solely on static access rules, this approach dynamically modifies access credentials based on user behavior, reducing the risk associated with insider threats.

Understanding the human factors that influence insider threats, such as employee motivations and vulnerabilities, can inform the development of more effective prevention and mitigation strategies.

In an era characterized by remote work and digital transformation, the need for robust strategies to identify and thwart insider threats within secure remote access models is paramount. To advance security and mitigate this ever-present risk, further research is required (Sarma, 2022). By delving into the nuances of user behavior, developing real-time monitoring solutions, and harnessing the power of AI and machine learning, researchers can make significant strides in addressing this pressing concern and enhancing the security of remote access to corporate networks. This, in turn, will contribute to the resilience of modern organizations in the digital age.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter goes into great detail about the research methodology. The study's methodology includes the research design, which serves as a guide for creating the model and outlining the design process. The research design also addresses the research methodology selected for this study. The data source, which explains the study's population, is also covered in this chapter. Information on data selection and sample techniques is also provided how the study will obtain the necessary consent to use the data for analysis.

It also includes data pre-processing, which is concerned with arranging the data and making sure that it is suitable for analysis. Data mining is also discussed, which explains how to utilize the SPSS program to gather information and do regression and predictive analytics. It also includes data transformation, which is the process of scaling up the data to the format needed for analysis. Data processing is another area covered by this, which relates to making sure that every piece of data is scaled to the format needed for analysis. Next, the test's output results are shown, accompanied by the resulting Knowledge Gap. The section on ethical considerations in this chapter describes how the study will secure the required authorization to utilize the results for analysis. The great County of Kericho was the site of this study.

Because of their adaptability and usefulness, a regression model was developed because it provides multiple advantages and it is frequently employed in various domains of study and practical applications. Regression models offer a powerful and adaptable framework for analyzing variable interactions, making predictions, and informing decision-making across a wide range of disciplines and businesses.

3.1 Design of the Study

The research design of this study was rooted in a quantitative research approach, which characterized by its emphasis on the measurement and analysis of numerical data to understand and draw conclusions about the research objectives. In this discussion, we delved into the key elements of the research design, data collection methods, sample size, survey questionnaire, and data analysis techniques.

A quantitative research approach was chosen to systematically collect and analyze numerical data that allowed for objective and statistical assessment of the study's objectives Dannels, 2018). This approach was particularly suitable for examining relationships, associations, and patterns among variables in a structured and systematic manner.

The study population comprises employees who access enterprise networks remotely within Kericho County. From this population, a sample size of 1200 employees were randomly selected. Random sampling ensures that each member of the population has an equal chance of being included in the study (Dannels, 2018). This approach helped in reducing bias and enhancing the generalizability of the findings.

The primary data collection tool for this study was a survey questionnaire. The survey questionnaire is a structured instrument that allows researchers to collect data from respondents in a standardized format. In this case, the questionnaires were administered to the selected employees. The survey questionnaire consisted of both closed-ended and open-ended questions.

These questions were designed to gather specific, quantifiable responses. Respondents were to select answers from predetermined choices. Closed-ended questions were used to objectively quantify variables and assess particular aspects of the research objectives. For

example, respondents were being asked to rate their satisfaction with remote access security on a scale from 1 to 5.

These questions were designed to elicit more detailed and qualitative responses. Respondents were encouraged to provide their thoughts and perspectives in their own words. Open-ended questions were used to capture additional data and insights beyond what can be obtained through closed-ended questions. For example, respondents were being asked to describe their experiences with remote access security challenges.

The evaluation and measurement of open questions in the study of secure remote access to enterprise networks involve qualitative analysis techniques aimed at uncovering patterns, themes, and insights within the responses. By systematically analyzing and interpreting qualitative data, researchers can gain valuable insights into the perceptions, experiences, and behaviors of stakeholders related to remote access security.

The generation of survey questions in the study typically involved a systematic process aimed at capturing relevant information, addressing research objectives, and ensuring the validity and reliability of the survey instrument. Defined research objectives and identified the key areas of inquiry. This involved understanding the specific aspects such as security measures, user behaviors, technological challenges, or organizational policies. Conducted a comprehensive literature review to identify existing research, theories, and frameworks relevant to secure remote access. Drafted questions based on the identified topics and themes, that align with the research objectives. Pilot test the survey instrument with a small sample of respondents to evaluate the clarity, relevance, and comprehensiveness of the survey questions. Refined the survey questions based on feedback from pilot testing and ongoing review by stakeholders. Once the survey questions were being refined and finalized, incorporated them into the survey instrument along with any necessary instructions or introductory text.

Once the survey data was collected, it was subjected to both descriptive and inferential statistical analyses:

Descriptive statistics, such as standard deviation, mean, and frequency distribution, were applied to summarize and characterize the survey data. Standard deviation measures the degree of variation within the data, the mean provided an average value, and frequency distribution presented a summary of response frequencies. These statistics help in understanding the central tendencies and distribution of responses.

Inferential statistics, included correlation and regression analysis, were used to investigate relationships and associations between variables in the study. Correlation analysis assessed the strength and direction of relationships between variables, while regression analysis helped predict the impact of one or more independent variables on a dependent variable.

The dissertation emphasizes ethical considerations to ensure the well-being and privacy of research participants. Informed consent was obtained from all participants, providing them with a clear understanding of the research's purpose and procedures. Confidentiality was maintained to protect the identity of respondents, and anonymity was preserved to prevent the disclosure of individual responses.

This quantitative research design relies on a structured survey questionnaire to collect data from a sample of 1200 employees in Kericho County. The study aimed at employing both descriptive and inferential statistical analyses to investigate remote access security and its various aspects. Ethical considerations played a crucial role in safeguarding the rights and privacy of research participants, ensuring the research was conducted with integrity and responsibility.

3.1.1 Data

Gathering data from the Kericho county database was a foundational step in the research process. Access to detailed information about teleworking and the types of businesses operating within the county was vital for constructing an accurate and representative model. This database contained a wealth of information regarding how teleworking was implemented, the various businesses involved, and other relevant contextual factors. Leveraging data from a local database was advantageous as it allowed for a focus on region-specific considerations, tailoring the research to the unique dynamics and circumstances of Kericho County. The insights gained from these data provided a valuable foundation for the study's modeling and analysis. Obtaining proper authorization from the relevant authorities in Kericho County was a critical ethical and procedural step. It demonstrated respect for legal and ethical protocols, ensuring that the research was conducted responsibly and in compliance with the necessary regulations. This authorization also signified collaboration and cooperation between the researchers and the local governing body, fostering a sense of community engagement and support for the research initiative.

Incorporating insights from published articles was a commendable practice. Published articles were valuable resources that provided a broader perspective on the subject matter. They often contained research findings, methodologies, and expert opinions, which helped enrich and validate the research being conducted. This integration of existing knowledge into the research process demonstrated a thorough and informed approach.

By combining data from the Kericho county database, proper authorization from authorities, and insights from published articles, the research benefitted from a well-rounded foundation. This approach allowed a comprehensive exploration of teleworking and its relationship with various types of businesses within the Kericho County context, leading to a more informed and robust research outcome.

Once the pilot test was complete, the required correction was undertaken, and a consent for data collection sought from the authorities. A formal letter of introduction from KCA University was obtained and served to introduce the researcher to the target population. Similarly, a letter of consent from Kericho county management was sought to ensure that the researcher has authority to access the respondents in their places of work. The questionnaires were administered through the human resources management in the different enterprise networks in the month of September 2023. Following the administering of the questionnaires, I followed up on the progress of filling the data collection instrument on a weekly basis. Finally, in early October 2023 the questionnaires were collected from the same human resources department after a period of three weeks had elapsed. The questionnaires collected were in a good state and clean hence ensuring that data recording and input was correct.

3.1.2 Sampling and Selection of Data

The sampling and selection of data for this study will involve a random sampling technique to select participants from the study population. The study population consisted of employees who access enterprise networks remotely. To ensure a representative sample, the study selected participants from different departments. Those who are available and were willing to engage in the study were chosen as participants.

Twenty people from each department make up the study's sample size. The formula for estimating the number of samples based on the number of participants and margins of error used to determine the sample size. The calculation was to have a 95% confidence level and a 5% margin of error. The study employed a method of stratified random sampling to choose the participants, in which the study's population were being separated into strata depending on various organizational sizes (Dannels, 2018). To guarantee that the sample accurately represented the total population, participants were chosen at random from each stratum. The participants invited to participate in the study voluntarily, and their participation was

anonymous and confidential. Informed consent was obtained from each participant before administering the survey questionnaire.

The sample frame outlines the members of the target population within the study. In the current study thesampling frame captures the employees of Kericho County. The total number of County staff members within Kericho County stands at 1200.

TABLE 3.1

Target Sample Population

Description	Population in Numbers
Senior staffs	209
Junior-level Staff	991
Total	1200

The exact sample size was determined using the Nassiuma's Formula as presented below:

$$n = \frac{NC^2}{C^2 + (N - 1)\, e^2}$$

Where: n = sample size

N=Population

C= coefficient of variation ($21\% \leq C \leq 30\%$),

e= the precision level ($2\% \leq e \leq 5\%$)

The formula was used to calculate the sample as shown;

$$n = \frac{1200 \times 0.25^2}{0.25^2 + (1200 - 1)\, 0.03^2}$$

$$n = 65.6973$$

$$n = 66 \text{ respondents}$$

3.1.3 Data Pre-processing and Transformation

Data pre-processing and transformation are critical steps in the analysis of any research study. In the data collected through the survey questionnaire underwent pre-processing and transformation before analysis.

The first step in data pre-processing was data cleaning, where the collected data was checked for any errors, inconsistencies, or missing values. Any inconsistencies and missing values were resolved through imputation, where the missing values were filled based on the available data.

After cleaning, the data was being transformed into a suitable format for analysis. This included scaling, normalization, and categorization of data. Scaling was used to bring the different variables to the same range, while normalization was used to ensure that the data followed a normal distribution. Categorization was used to group the data into categories for analysis.

The next step was data reduction, which involved reducing the amount of data to manageable sizes. This was done through techniques such as principal component analysis (PCA) and factor analysis. These techniques helped to reduce the number of variables and simplify the analysis process.

After data reduction, the transformed data was being analyzed using statistical techniques such as descriptive statistics, correlation analysis, and regression analysis. Descriptive statistics were used to summarized the data, while correlation and regression analysis were being used to identify the relationships between the different variables.

Following data reduction, statistical methods including correlation analysis, descriptive statistics, and regression analysis were used to examine the modified data. The data was summarized using descriptive statistics, and the relationships between the various variables were found using correlation and regression analysis.

Finally, the results obtained from the data analysis were interpreted to answer the research questions and objectives. This interpretation helped to draw conclusions and provides recommendations for the study.

3.1.4 Data Mining

This procedure involved providing inputs to the model for processing, allowing it to be trained on the types of input data and the anticipated outcome of the training session. The data was maintained within an Excel data sheet. This data was subjected to machine learning algorithms and statistical models. Subsequently, the Excel sheet was saved in a format that enabled it to be read by the statistical program R. To maximize productivity when dealing with the data, the data was initially scaled to fit within a [0, 1] interval after being imported into the R software (Dannels, 2018). This scaling process standardized the data, making it more amenable to further analysis and enhancing the efficiency of data handling within the R environment.

The data underwent a partitioning into a 70:20 ratios. Approximately 80% of this split was designated as the training dataset, while the remaining 20% was allocated as the test dataset. This approach allowed for training the model on a significant portion of the data while reserving a distinct portion for evaluation. 70% of the data was utilized for training, ensuring a sufficiently large dataset to train the model effectively. The remaining 30% of the data served as the test set, providing a separate and untouched dataset to assess the model's performance, generalization, and predictive capabilities.

Moving forward, the training data, constituting 80% of the data, was fed into the Artificial Neural Network (ANN) model through the identified model neurons. The ANN model leveraged these neurons to process the training data and optimize its parameters through a series of training rounds. During this process, the ANN algorithm iteratively adjusted its weights based on the training data to improve performance (Dannels, 2018).

To thoroughly evaluate the ANN model's performance, three distinct neural network algorithms were put to the test, each employing different activation functions. These activation functions included logistic activation, linear activation, and ReLu (Rectified Linear Unit) activation. These different algorithms were explored to assess how different activation functions influenced the performance and outcomes of the model, enabling a comprehensive understanding of the ANN's capabilities and behavior.

3.1.5 Validity Test

In the realm of research, the accuracy and effectiveness of the research instrument used to collect data are of paramount importance. Ensuring that the instrument accurately measures the intended objects and provides reliable information is essential for the success and credibility of any study. In this discussion, we explored the concept of content validity, the methods employed to establish it, and the significance of Kaiser-Meyer-Olkin (KMO) and Bartlett's Test of Sphericity in the validation process.

Content validity was a critical aspect of research instrument validation. It refered to the extent to which the instrument accurately measures the concept or constructs it is designed to assess. In other words, a research instrument is said to have content validity when it comprehensively and faithfully captures the essence of what it intended to measure (Dannels, 2018).

In the context of this research study, content validity was rigorously established to ensure that the research instrument effectively captured the intended variables and provided accurate information about the research objectives. The following steps were taken to assess and confirm content validity:

This result is significant because it affirms that the research instrument used for data collection is capable of effectively capturing the underlying factors and relationships within the data. The KMO test helps establish the instrument's content validity by confirming that the variables are interrelated and suitable for in-depth analysis.

Bartlett's Test of Sphericity complements the assessment of content validity by evaluating whether factor analysis is appropriate for the dataset. This test assesses whether the variables are related and whether they exhibit patterns that can be analyzed together. Significance in Bartlett's Test of Sphericity, typically indicated by a p-value of less than 0.05, suggests that the data is suitable for factor analysis.

In the study, the results of Bartlett's Test of Sphericity indicate a significance level of less than 0.05. This outcome is crucial because it confirms that the dataset is suitable for factor analysis. In essence, the test reinforces the content validity of the research instrument by confirming that the data exhibits the required relationships and patterns necessary for thorough analysis.

Content validity, as established through the KMO and Bartlett's Test of Sphericity, is a foundational aspect of research quality. It ensures that the research instrument effectively captures the intended variables and provides reliable information for the study's objectives. When content validity is confirmed, researchers can have confidence in the instrument's ability to measure and assess the constructs of interest accurately.

The content validity is a critical component of research instrument validation. The study's rigorous approach to establishing content validity through the KMO and Bartlett's Test of Sphericity demonstrates the instrument's capability to accurately measure the intended variables. This validation process is pivotal in ensuring the research's credibility and the reliability of the data collected.

TABLE 3.2

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.788
Bartlett's Test of Sphericity	Approx. Chi-Square	656.71
	df	200
	Sig.	<.001

The KMO test is a statistical measure used to evaluate the sampling adequacy and suitability for factor analysis. It assesses whether the variance in the variables can be attributed to underlying factors. A KMO value close to 1.0 is highly desirable, as it indicates that the variables are sufficiently related and that they can be effectively analyzed together. In the case of the study, Table 3.2 demonstrates that the KMO value exceeds 0.5, suggesting that the sample size is adequate for factor analysis.

3.1.6 Reliability Test

In the realm of research, ensuring the reliability of a research instrument is an essential step that cannot be overlooked. Reliability refers to the degree of internal consistency and dependability of a research instrument, ensuring that it produces consistent and replicable results when administered to different samples from the same target population (Scott, 2019). The internal consistency of a research instrument is a fundamental attribute that researchers seek to establish to ensure the credibility and validity of their findings. This discussion explores

the importance of reliability testing and the use of the Cronbach's Alpha test in the research process.

Reliability testing plays a pivotal role in the research process as it evaluates the extent to which the research instrument is dependable and internally consistent. In other words, it seeks to answer the question: Can the research instrument consistently yield similar results when administered to different individuals from the same population?

The primary goal of reliability testing is to minimize errors and inconsistencies in the research data. If a research instrument is unreliable, it can introduce bias, inaccuracies, and inconsistencies in the findings, ultimately undermining the credibility of the research. Therefore, establishing the internal consistency of the instrument is of paramount importance.

To assess the internal consistency and reliability of the research instrument, the study utilized the Cronbach's Alpha test. Cronbach's Alpha is a widely accepted statistical measure used to evaluate the extent to which the items within a questionnaire or survey are interrelated and produce consistent results when measuring a specific construct or concept.

In the context of the study, the Cronbach's Alpha test was employed to determine whether the questionnaire produced consistent and dependable results when administered to different samples from the same target population. The test provides a numerical value, known as Cronbach's Alpha coefficient, which ranges from 0 to 1.

Value Greater than 0.7: A Cronbach's Alpha coefficient greater than 0.7 is generally considered a strong indicator of reliability. It signifies that the research instrument exhibits a high level of internal consistency, and the items within the instrument are closely related, contributing to the consistent measurement of the intended construct.

Value Below 0.7: Conversely, a Cronbach's Alpha coefficient below 0.7 suggests that the research instrument may lack sufficient internal consistency. In such cases, it is crucial to

review and refine the instrument to enhance its reliability. This could involve revising or eliminating problematic items or reevaluating the instrument's design.

Reliability testing is instrumental in ensuring that the research instrument functions as intended. By confirming the internal consistency of the instrument, researchers can trust that it will consistently measure the constructs under investigation. This, in turn, enhances the validity and credibility of the research findings.

The reliability test, as assessed through the Cronbach's Alpha test, is a critical step in the research process. It serves as a quality assurance measure, ensuring that the research instrument produces consistent and dependable results. By establishing internal consistency, researchers can have confidence in the instrument's ability to accurately measure the variables of interest, ultimately contributing to the reliability and validity of the research.

TABLE 3.3

Reliability Analysis

Variable	Test Items	Alpha Values
Technology	7	0.765
Organizational Factors	4	0.736
Employees	8	0.757
Monitoring & Evaluation	6	0.788
Resource Management & Controls	5 4	0.756 0.738
Data Protection & Monitoring		

A comprehensive pilot study was undertaken with a view of determining the reliability of the questionnaire. Using the Cronbach Alpha metric, the internal consistency of the questionnaire was determined and it established that the four study variables questions were reliable. According to table 3.2, Technology had a reliability of 0.765; Organizational Factors 0.736; Employees 0.757; Monitoring & Evaluation 0.788; Resource Management & Controls

0.756; Data Protection & Monitoring had a reliability of 0.738. Since the study variables had alpha values exceeding 0.7, the questionnaire was deemed as reliable.

3.1.6 Model Evaluation

This procedure was a standard practice in machine learning and modelling. It involved using a test information set to assess whether a model has been effectively trained. This was done by comparing the actual output produced by the model with the expected output. In essence, the model's performance is evaluated against known data to ensure it was making accurate predictions.

During the evaluation, any differences between the actual and expected results are quantified using error metrics. These error metrics help identified the shortcomings of the model and areas where it needs adjustment. The research study used these metrics to fine-tune the model's weights, often through an iterative process, utilizing a validation data set. The goal is to minimize the error rate, ensuring that the model's predictions align as closely as possible with the expected outcomes.

The training process is not a one-time event but rather an iterative one. The study conducted multiple trials to refine the model's output data. In each trial, the model was adjusted to optimize its performance. This iterative approach ensures that the most appropriate weights for each input are determined, leading to a highly accurate and reliable model.

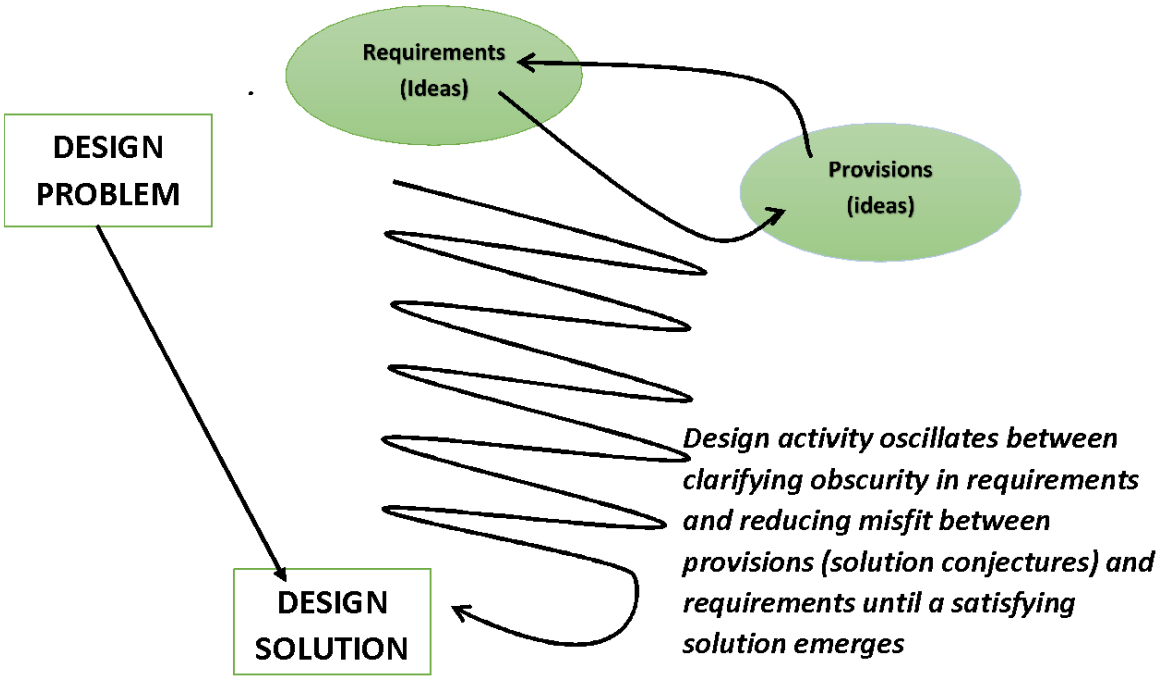
The information concludes by mentioning that the research's outcomes are presented at the Knowledge Gap. This implies that the research findings and model developed will be shared, presumably to address or fill a specific knowledge gap in the field. This is an important step in disseminating research findings and contributing to the collective body of knowledge in the relevant area of study.

3.2 Model Development Framework

To create and develop the Model, the study employed a create Science Research methodology. The reason is that it works well with IT-based research because it employs systematic processes that allow one to return to an earlier stage at any moment to assess the artifact in light of newly discovered information. According to McKay et al. (2021), a diagrammatic overview of design science is shown below.

FIGURE 3.O

Design Construct in Information Systems Design Science



To create and develop the Model, the study employed a Design Science Research methodology. The reason is that it works well with IT-based research because it employs systematic processes that allow one to return to an earlier stage at any moment to assess the

artifact in light of newly discovered information. According to McKay et al. (2021), a diagrammatic overview of design science.

3.3 Data Processing and Analysis

The study utilized Microsoft Excel for data analysis. Excel is a commonly used tool for data analysis, offering a wide range of functions and capabilities for processing and interpreting survey data. The use of Excel allowed for the manipulation, calculation, and visualization of data, making it an effective choice for this purpose.

The study employed newly created Google Forms for survey distribution. This approach is especially relevant, considering the challenges posed by the COVID-19 pandemic. Using digital surveys via Google Forms eliminates the need for physical forms, which can be risky during a health crisis. It offered a safer and more convenient way to collect responses from participants. Google Forms were noted for their use of graphical representations such as pie and bar graphs to present survey results. This visualization approach can be highly effective for conveying survey findings in an accessible and user-friendly manner. Graphical representations made it easier for both researchers and stakeholders to grasp key insights from the data.

The study employed model validation as a process to ensure that the design complies with information security requirements. Model validation is a crucial step in assessing the effectiveness and suitability of a model. In this context, the study aimed to confirm that the model developed for remote access security aligns with the specific information security needs and standards of the county. Feedback from stakeholders and end-users was utilized to evaluate the model's viability and its capacity to deliver the desired performance. This feedback-driven approach ensures that the model is practical, effective, and aligned with the actual needs of the

county. It also addresses whether the model can effectively support secure remote access to corporate networks.

The study's methods demonstrate a comprehensive and technology-driven approach to data collection, analysis, and model validation. Leveraging digital tools like Google Forms for data collection and MS Excel for analysis streamlines the research process and provides efficient means of presenting survey results. Additionally, the focus on model validation and stakeholder feedback ensures that the solutions and recommendations offered in the study are practical, secure, and relevant to the specific requirements of the county, emphasizing the importance of information security in the context of remote access to corporate networks.

The quantitative data was analysed in order to come up with findings and conclusion. Once the questionnaires were returned, the researcher utilized the Statistical Package for Social Sciences (SPSS v27) to analyse the data. The data was analysed using inferential statistics. The inferential statistics included correlation statistics and multiple regressions analysis. Multiple regressions is an example of ordinary least-squares model since it entails multiple explanatory variables. The multiple regressions function used in the study is illustrated below:

$Y= \beta 0 + \beta 1X1+ \beta 2X2+ \beta 3X3+ \beta 4X4+ \beta 5X5+ \beta 6X6 +\varepsilon$ Where:

Y	=	Remote Access Security
β0	=	Constant
X1	=	Technology
X2	=	Organizational factors
X3	=	Employees
X4	=	Monitoring & Evaluation

X5	=	Resource Management & Controls
X6	=	Data Protection & Monitoring
ε	=	Error Term
β1,β2,β3,β4,β5,β6	=	Regressions Coefficients

CHAPTER FOUR

FINDINGS AND DISCUSSION

4.0 Introduction

This chapter describes the findings of an empirical study done in Kericho County to evaluate the paradigm of secure remote access to company networks by employees. The information was gathered using a combination of surveys distributed to county personnel, database analysis, and a review of relevant publications. This chapter presents the findings in detail, followed by a thorough discussion of these findings in the context of the research aims and previous literature.

4.2 Demographic Profile of Respondents

Demographic Profile of Respondents indicates that the poll conducted in Kericho County aimed to collect a wide range of perspectives by including employees from various departments, genders, age groups, employment positions, and years of service. This diversity in respondent demographics is important for a comprehensive understanding of the issues being surveyed and how different segments of the employee population perceive them.

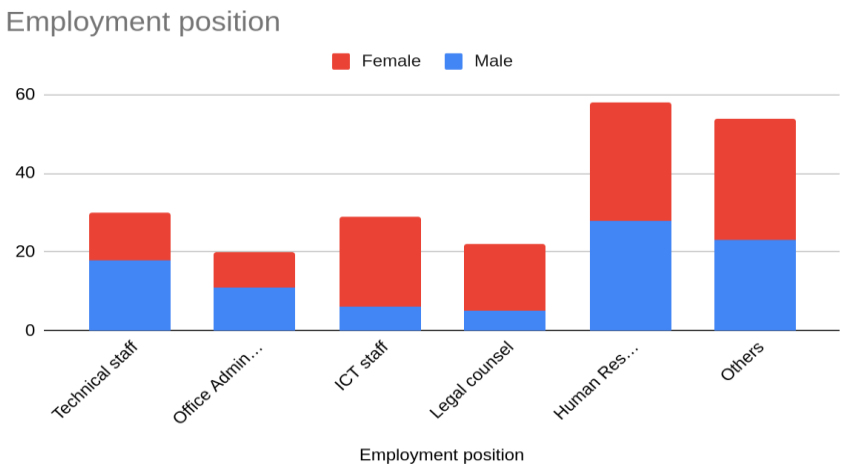
The poll received responses from a wide and diverse group of employees who work for Kericho County. This suggests that the survey aimed to include input from a broad cross-section of the organization rather than focusing on a specific subset of employees.

The respondents came from different departments and performed various functions or roles within the county. In a large organization like a county government, there are typically multiple departments such as ICT, legal counsel, technical staff, public works, health, and so on, each with its own set of functions and responsibilities. This implies that the survey sought input from employees across these different areas.

The survey collected responses from individuals of different genders. This could include male and females. Understanding the gender distribution among respondents can provide insights into how different gender groups within the organization perceive or respond to the issues addressed in the survey. As shown below:

FIGURE 4.1

Employers Position at Kericho County



The respondents held various job titles or positions within the organization. These positions could range from entry-level roles to managerial or leadership positions. Examining the distribution of respondents across different job roles allows for a better understanding of how different parts of the organization are represented in the survey results.

From the questionnaire distributed to the participants there was 92.4 percent response.

TABLE 4.1

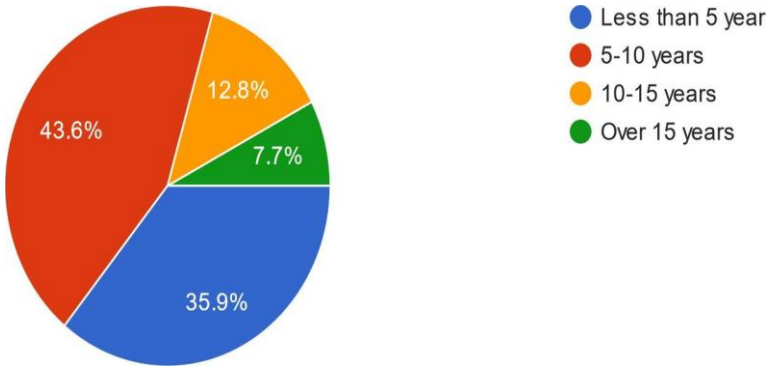
Participants

	Questionnaires Administered	Questionnaires filled & Returned	Percentage
Respondents	66	61	92.42 %

The table presents data on questionnaire administration and response rates. Out of 66 questionnaires administered, 61 were filled and returned**,** resulting in a high response rate of 92.42%**.** This indicates strong participant engagement and reliability in data collection.

FIGURE 4.2

Participants Years of Employment at Kericho County



Pie chart, shows the characteristics of the participants who answered the questions from the questionnaire distributed. 7.7 % of them have been working in Kericho county for over 15 years, 12.8% have been working for 10-15 years, 43.6% have been working for 5-10 years and 35.9% have been working for less than 5 years. The respondents had different years of service with Kericho County. This information helps in categorizing employees based on their experience within the organization, such as 0-5 years 5-10 years, 10-15 years, and 15-30 years. The years of service can influence an employee's familiarity with the organization's culture and operations.

TABLE 4.2

Participants' Characteristics

	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 County Offices	28.2 %	33.3 %	17.9%	17.9%	2.6%	2.33	1.15

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 departments around them while working from home, while the rest have no people in the county around them while working remotely.

4.3 Research Findings

4.3.0 Objective One Results

The research study embarked on a crucial journey with its primary objective: to comprehensively identify the security risks that arise when employees access organizational networks remotely. Specifically, it aimed to shed light on the inadequacies of conventional security measures in effectively countering these emerging threats within the context of Kericho County. This objective was not merely a theoretical endeavor; it was a practical exploration into the real challenges faced by organizations in the digital age as remote work becomes increasingly prevalent.

In pursuit of this objective, the research delved into the multifaceted landscape of security risks associated with remote employee access. The intention was to uncover the intricacies of these threats and understand the nuances that set them apart from traditional security concerns. By focusing on Kericho County, the study aimed to offer a localized perspective that could be applicable to organizations operating in similar environments.

To fulfill this objective, the research team designed and administered a questionnaire to a sample of respondents. This questionnaire served as a valuable tool for gathering firsthand insights from those who are directly involved in remote work scenarios within the county. It was through this data collection process that the research began to unravel the major security challenges that organizations and their employees face. These challenges, as reported by the respondents, serve as a critical foundation for understanding the security landscape in the context of remote access.

The findings of the research, as illuminated by the respondents' feedback, highlighted several principal challenges in the realm of remote employee access security. These challenges

have significant implications for organizations seeking to safeguard their digital assets and sensitive information:

Inadequate Authentication Protocols: One of the foremost challenges identified was the inadequacy of traditional authentication methods in ensuring the security of remote access. Respondents revealed concerns regarding the susceptibility of password-based authentication to breaches and unauthorized access.

The research brought to the fore the heightened concerns about data privacy. In the age of remote work, the protection of sensitive data during transmission and storage became a critical issue, prompting organizations to rethink their data protection strategies.

The security of remote devices emerged as a key concern. Ensuring that the devices used by employees to access corporate networks are adequately protected against malware, intrusions, and other threats became a top priority.

The study exposed the vulnerabilities inherent in remote network connections. It underscored the significance of securing the pathways through which remote access is granted, including virtual private networks (VPNs) and secure communication protocols.

Respondents articulated the need for comprehensive training and awareness programs. As remote work became more prevalent, organizations had to address the gaps in knowledge and awareness regarding secure remote access practices among their employees.

The research's first objective laid the groundwork for understanding the security challenges faced by organizations in Kericho County as they embraced remote work. By tapping into the experiences and perspectives of those directly involved, the study illuminated critical areas where conventional security measures fell short in the face of evolving threats. These findings are instrumental in guiding organizations toward more effective security strategies and practices that are aligned with the demands of the digital age. They serve as a

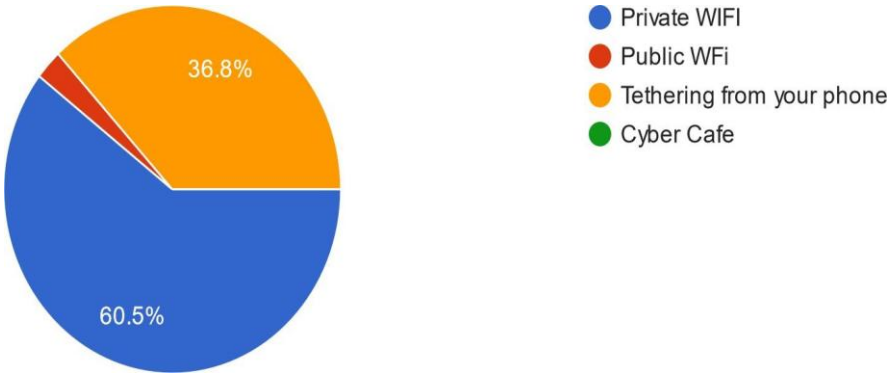
testament to the research's commitment to addressing real-world challenges and contributing to the advancement of security in the context of remote employee access to corporate networks.

4.3.1 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.

FIGURE 4.3

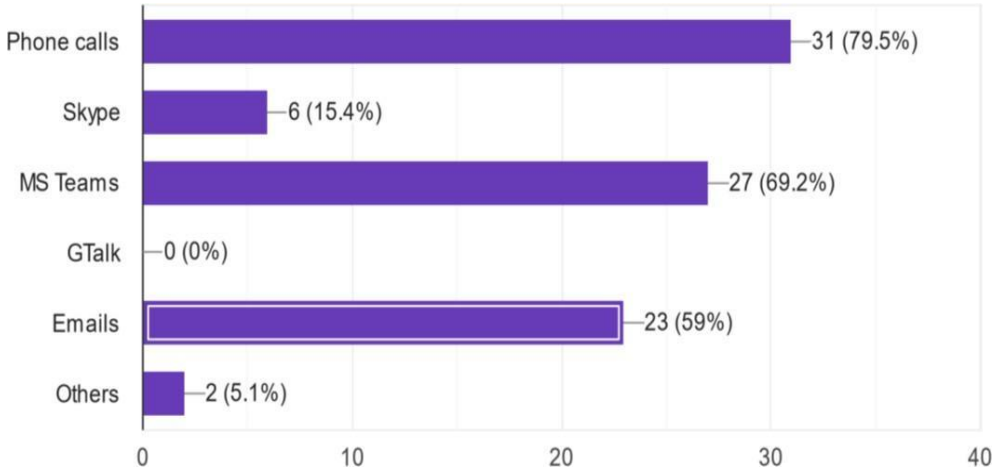
Source of Internet while Teleworking



The pie chart illustrates the distribution of internet access methods used. The majority of users (60.5%) rely on Private WiFi for internet access. Tethering from a phone follows with 36.8%, while a smaller percentage access the internet via Public WiFi and Cyber Cafes, both showing minimal usage.

FIGURE 4.4

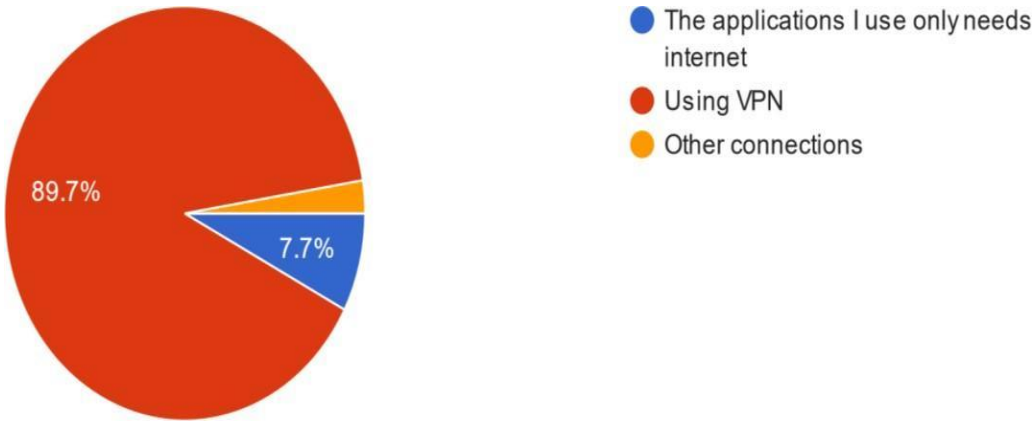
Mode of Communication



The bar chart depicts the communication methods used, with Phone calls being the most utilized at 79.5% (31 users), followed closely by MS Teams at 69.2% (27 users) and Emails at 59% (23 users). Skype is used by 15.4% (6 users), while Others account for 5.1% (2 users). Notably, GTalk recorded no usage (0%). This highlights a preference for phone-based and collaborative communication tools over other methods.

FIGURE 4.5

Mode of Connecting to the Office Network



The pie chart illustrates the types of internet connections used by participants. A significant majority **(**89.7%**)** rely on VPN connections, while **7.7%** use applications that

require only the internet. A small fraction represents other connections, highlighting alternative methods for accessing resources.

TABLE 4.3

Technology Controls in Place

	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%

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 machine 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 threats. 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 staffs to have visibility of who is teleworking and what they are doing.

4.3.2 The Organizational Aspect in Information Security

In the pursuit of a thorough understanding of information security within the realm of teleworking, the research extended its scope to encompass the critical organizational dimension. This exploration was driven by the imperative to gauge the extent to which the organization had implemented measures and protocols aimed at safeguarding corporate information when employees engage in teleworking activities.

The organization's preparedness and commitment to information security form a crucial pillar in ensuring the integrity and confidentiality of sensitive corporate data. The study acknowledged that in the contemporary digital landscape, characterized by remote work and the dynamic exchange of information, organizations must proactively address the security challenges presented by teleworking.

Central to this organizational preparedness is the presence and effectiveness of information security policies. These policies serve as a roadmap for employees and stakeholders, guiding them on the best practices, protocols, and expectations concerning the security of corporate information. In the context of this study, the organization under examination was found to have such a policy in place.

The research unearthed a noteworthy facet of the organization's approach to information security: the annual update of its information security policy. This practice underscores the organization's commitment to maintaining the relevance and effectiveness of its security measures in the face of evolving threats and changing circumstances.

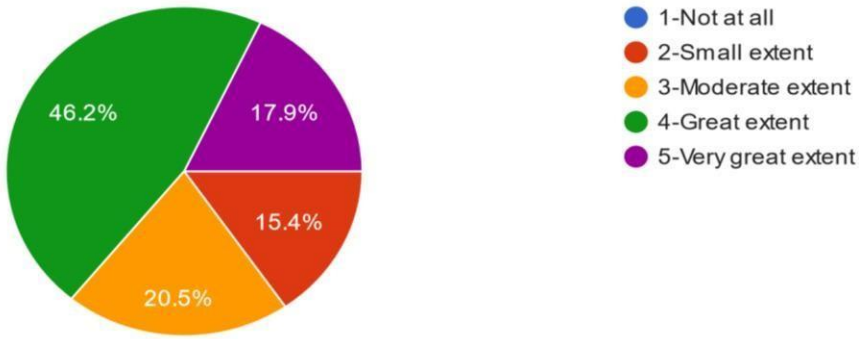
Notably, the research highlighted another vital attribute of the organization's information security policy – accessibility. The policy was designed to be easily accessible to

all employees. This accessibility is instrumental in ensuring that every member of the organization, regardless of their role or department, has the means to familiarize themselves with the security protocols and guidelines outlined in the policy.

In the context of teleworking, where remote access to corporate networks is prevalent, this commitment to annual updates and accessibility ensures that all employees are aware of the evolving security landscape and the measures they need to undertake to protect corporate information.

FIGURE 4.6

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.

TABLE 4.4

Information Security Policy

	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%

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 4.7

Type of Access to Systems while Teleworking

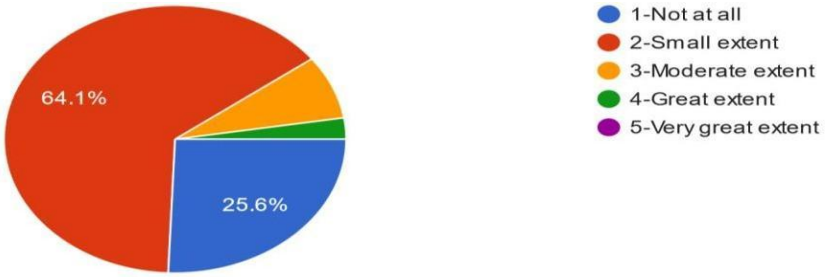
All employees have restricted access to the systems while teleworking and access to the systems is only given on request when required this mainly happens during working days. However, staff from ICT have full access for support purposes.

4.3.3 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 is power and internet down time.

FIGURE 4.8

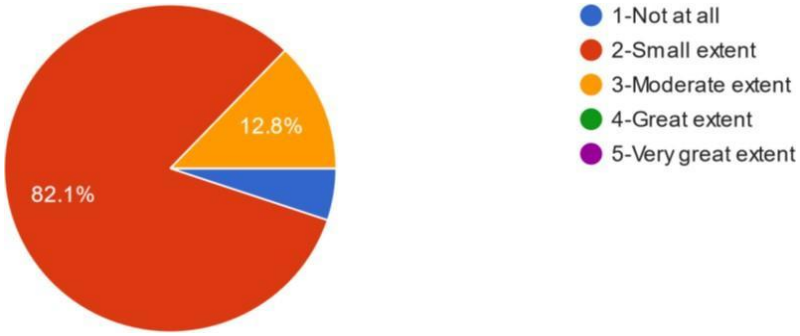
Power Outage While Teleworking



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 4.9

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 sources. Only 35% do not do not have a backup for the internet.

4.4. Objective Two

The second objective of the research study was to investigate the many security mechanisms, such as user authentication, access control, data encryption, intrusion detection and prevention, and secure communication protocols that can be used to safeguard remote access.

The analysis of the organizational database emphasizes the importance of secure remote access, particularly during times of crisis like the COVID-19 epidemic. This involved reviewing data related to remote access, including how employees access company resources and data remotely. The analysis has drawn attention to the critical importance of secure remote access. Secure remote access means that employees can access company systems and data from outside the traditional office environment while ensuring that the data remains protected from security threats and breaches. The results for the second objective are illustrated in table 4.5.

TABLE 4.5

Results for Objectives Number 2

Variable	B	Significance
(Constant)	2.683	0.000
Technology	0.112	0.000
Organizational Factors	0.211	0.000
Employees	0.309	0.000
Monitoring & Evaluation	0.241	0.000
Resource Management & Controls	0.213	0.000
Data Protection & Monitoring	0.107	0.000

Subsequently, following the analysis, the researcher established that technology, organizational factors, employees, monitoring and evaluation, resource management and controls, and data protection and monitoring are statistically significant in the attainment of a Remote Access Security to Enterprise Networks by Employees, the table indicates that as the constant with a B value of 2.683 and a significance level of 0.000 likely represents the intercept or the baseline level of achieving secure remote access when all other variables are zero. Technology variable has a B value of 0.112 and a significance level of 0.000. This indicates that technology has a positive relationship with achieving secure remote access, and the

relationship is statistically significant. In other words, technology is an important factor in achieving secure remote access. Organizational Factors has a B value of 0.211 and a significance level of 0.000. This suggests that organizational factors also have a positive and statistically significant impact on achieving secure remote access. These factors related to the organization contribute to the outcome. Employee variable has a B value of 0.309 and a significance level of 0.000. This shows a positive and statistically significant relationship between employees and the attainment of Remote Access Security. Employee-related factors are important for achieving security. Monitoring & Evaluation: This variable has a B value of 0.241 and a significance level of 0.000. It is positively related and statistically significant, meaning that monitoring and evaluation processes play a crucial role in achieving remote access security. Resource Management & Controls: With a B value of 0.213 and a significance level of 0.000, resource management and controls are positively and significantly related to achieving remote access security. Efficient resource management and control practices contribute to security. Data Protection & Monitoring: This variable has a B value of 0.107 and a significance level of 0.000. It's also positively related and statistically significant, indicating that data protection and monitoring are important for achieving remote access security.

The table's summary suggests that all the listed factors are statistically significant in achieving secure remote access to enterprise networks by employees. This means that these factors play a meaningful role, and their influence on the outcome is not due to random chance. The positive coefficients also imply that an increase in these factors is associated with a higher likelihood of achieving remote access security. Researchers and decision-makers can use this information to prioritize and focus on these factors when aiming to enhance the security of remote access to enterprise networks by employees.

The research findings underscore the imperative of establishing a robust infrastructure and well-defined procedures to facilitate remote work while concurrently upholding data

security. In today's dynamic work environment, remote work has become an integral component of organizational operations, necessitating a comprehensive approach to safeguarding sensitive data. The analysis indicates that organizations must proactively implement a suite of infrastructure and procedures to support remote work effectively while maintaining the highest standards of data security. These essential components encompass a range of strategies and measures aimed at fortifying information security in the remote work environment.

Implementing a VPN is a cornerstone of secure remote work. VPNs provide encrypted and secure connections for remote employees accessing the organization's network. By encrypting the data transmitted over these connections, VPNs ensure that information remains confidential and protected from interception, thereby safeguarding sensitive data.

Requiring MFA as an authentication method adds an additional layer of security by confirming the identity of users accessing systems remotely. MFA can encompass various factors, such as something the user knows (password), something the user has (a smart card or token), and something the user is (biometric data). This multifaceted approach enhances access security by demanding multiple forms of verification.

Ensuring that data transmitted between remote locations and the organization's network is encrypted is paramount. Data encryption protects information from interception and unauthorized access during transit. Robust encryption measures provide an additional shield for sensitive data.

Developing and enforcing policies and procedures specific to remote work is essential. These guidelines should outline how remote work should be conducted, emphasizing best practices for data access and handling. Clarity in procedures ensures that employees are aware

of the expectations and requirements for remote work, contributing to a secure working environment.

Regular security audits are vital to identify vulnerabilities and assess the overall security of remote access systems. Periodic assessments help organizations stay ahead of emerging threats and vulnerabilities, allowing for timely adjustments and enhancements to security measures.

Enforcing strong password policies and implementing password management tools are foundational elements of information security. Strong, unique passwords, and efficient management tools minimize the risk of unauthorized access to systems and data.

Employing antivirus and anti-malware software is essential to protect against malicious software and cyber threats. Regular updates and maintenance of these tools are crucial to ensure ongoing protection.

Regular cybersecurity training and awareness programs for employees are imperative discussed by (Bourne, 2022). By keeping employees informed about evolving threats and best security practices, organizations empower their workforce to act as a front line of defense against potential security breaches.

Implementing monitoring systems to track user activities and the use of data loss prevention measures further bolsters security. These measures can identify potentially risky behaviors and safeguard data from unauthorized dissemination.

Conducting thorough background checks on employees and establishing clear security policies are fundamental. Background checks help ensure the trustworthiness of employees with access to sensitive data, while clear policies set expectations for security practices and procedures.

The research findings illuminate the critical need for organizations to adopt a multi-faceted approach to secure remote work while preserving data security. By implementing the recommended infrastructure and procedures, organizations can create a robust framework for remote work that ensures the confidentiality and integrity of sensitive data. This comprehensive approach enhances security and empowers organizations to navigate the evolving digital landscape with confidence and resilience.

4.5 Objective Three Results

The objective was to develop a security model for remote access to enterprise networks by employees, incorporating the identified security measures and utilizing VPN technology. Regression is a statistical technique used for binary classification problems, where the goal is to predict one of two possible outcomes. In the context of security, this often means classifying an event as either a security threat (1) or no threat (0). It's a popular choice for such problems because it provides probabilities as outputs, making it interpretable.

Regression, in contrast to conventional linear regression, forecasts probabilities of specific outcomes rather than continuous values. In this instance, it determines the likelihood that employees will have secure remote access to corporate networks. Regression, in contrast to conventional linear regression, forecasts probabilities of specific outcomes rather than continuous values. In this instance, it determines the likelihood that employees will have secure remote access to corporate networks. As presented below:

$Y= \beta0 + \beta1X1+ \beta2X2+ \beta3X3+ \beta4X4+ \beta5X5+ \beta6X6 +\varepsilon$ Where:

Y	=	Secure Remote Access
β0	=	Constant
X1	=	Technology
X2	=	Organizational Factors
X3	=	Employees

X4	=	Monitoring & Evaluation
X5	=	Resource Management & Controls
X6	=	Data Protection & Monitoring
ε	=	Error Term
β1, β2, β3, β4, β5,β6	=	Regressions Coefficients

Therefore, Secure Remote Access= 2.683+0.112 Technology+0.211 Organizational Factors+0.309 Employees+0.241 Monitoring & Evaluation+0.213 Resource Management & Controls+0.107 Data Protection & Monitoring.

The developed model shows that technology, organizational factors, employees, monitoring & evaluation, resource management & controls and data protection & monitoring have a significant association with Remote Access Security to Enterprise Networks by Employees in Kericho County. Subsequently, changes in the value of the variables affect Remote Access Security.

4.6 Objective Four Results

The fourth objective of the research study was to evaluate the effectiveness of the proposed security model in providing comprehensive and effective security measures for remote access security to enterprise networks by employees, and to identify areas for further improvement. Subsequently, Model Summary and ANOVA were used. The researcher developed an OLS model using multiple regressions totest the impact of the predictor variables on the dependent variable. Subsequently, SPSS v27 was used to input, code, and compute multiple regressions statistics. The model summary is illustrated in table 4.5.

TABLE 4.6

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.688[a]	0.673	0.634	0.228

a. Predictors: Constant, Technology, Organizational Factors, Employees, Monitoring & Evaluation, Resource Management & Controls, and Data Protection & Monitoring.

R: This represents the correlation coefficient (R), which is a measure of the strength and direction of the linear relationship between the dependent variable (Remote Access Security) and the combination of independent variables (Technology, Organizational Factors, Employees, Monitoring & Evaluation, Resource Management & Controls, and Data Protection & Monitoring). In this case, R is 0.688, which suggests a moderate positive correlation between the independent variables and remote access security.

R Square%: The R-squared value, often represented as a percentage, indicates the proportion of the variance in the dependent variable (Remote Access Security) that is explained by the independent variables. In this case, the R-squared value is 0.673, or 67.3%. This means that approximately 47.3% of the variability in remote access security can be explained by the combination of the listed independent variables.

Adjusted R Square%: The adjusted R-squared value takes into account the number of independent variables in the model, and it adjusts the R-squared value accordingly. It's a more conservative estimate of how well the independent variables explain the variance in the dependent variable. In this case, the adjusted R-squared value is 0.634, or 63.4%. It's very close to the R-squared value, which suggests that the model is relatively robust, even after accounting for the number of independent variables.

Std. Error of the Estimate: This is a measure of how well the model's predictions match the actual data. A smaller value indicates that the model is a better fit for the data. In this case, the standard error is 0.228.

The model summary indicates that the combination of independent variables (Technology, Organizational Factors, Employees, Monitoring & Evaluation, Resource

Management & Controls, and Data Protection & Monitoring) explains about 62.8% of the variation in Remote Access Security. This suggests that these factors collectively have a moderate level of influence on remote access security.

The adjusted R-squared value is 0.634, which means that after adjusting for the number of independent variables, the model still explains a significant portion of the variation in remote access security. The standard error of the estimate (0.228) is a measure of the model's accuracy in predicting the dependent variable. A lower standard error indicates that the model's predictions are closer to the actual values.

TABLE 4.7

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	76.914	152	0.878	50.731	0.000[b]
	Residual	6.357	48	0.123		
	Total	83.271	218			

Dependent Variable: Remote Access Security

Predictors: (Constant), Technology, Organizational Factors, Employees, Monitoring & Evaluation, Resource Management & Control, Data Protection & Control

This is the sum of squared differences between the observed values of the dependent variable Remote Access Security and the predicted values from the regression model. In this case, the sum of squares for the regression component is 76.914. df represents the degrees of freedom associated with the regression component. In this case, it's 170 degrees of freedom. The mean square is the sum of squares divided by its degrees of freedom. In this case, it's 0.878. The F-statistic is a measure of how well the independent variables collectively explain the variation in the dependent variable. A larger F-statistic indicates a better fit of the model. Here,

the F-statistic is 50.731. This represents the p-value associated with the F-statistic. A low p-value (typically below 0.05) suggests that the model is statistically significant. In this case, the p-value is very close to zero (0.000), indicating that the regression model is highly statistically significant.

The sum of squared differences between the observed values and the values predicted by the regression model. In this case, the sum of squares for the residuals is 6.357. The df associated with the residuals. It is 48 degrees of freedom. The mean square for the residuals is 0.123.

Sum of Squares: The total sum of squares represents the total variation in the dependent variable, including both the variation explained by the model (regression) and the unexplained variation (residuals). In this case, the total sum of squares is 83.271. The degrees of freedom for the total variation is 200 degrees of freedom.

The ANOVA table is a critical component of regression analysis. It helps assess the overall statistical significance of the model and whether the independent variables collectively have a significant impact on the dependent variable (Remote Access Security). In this case, the ANOVA results are highly significant. The p-value (Sig.) associated with the F-statistic is very close to zero (0.000), indicating that the regression model, with the listed independent variables, collectively has a significant effect on Remote Access Security.

A model summary of the logistic model discussed by Ernest Yeboah Boateng and Daniel A. Abaye, It could be observed that the model has a relatively larger R2 of 0.673 as compared with the Nagelkerke R2 0.576 (Ernest Yeboah Boateng and Daniel A. Abaye, 2019) . Linear regression model with an R-squared of 0.673 outperforms this existing logistic regression model in terms of explaining the variability in the outcome variable (remote access security). The higher R-squared value suggests that linear regression model captures a larger

proportion of the variance in remote access security compared to the logistic regression model. The Summary model table for message content logistic regression model table gives the values for two pseudo R2 (Cox & Snell R-Square and Nagelkerke R-Square) values, which can be interpreted in a similar way as coefficient of determination in regression models. The two pseudo R2 values measure the extent to which explanatory explains the variation in the dependent variable. The two pseudo R2 were; 0.112 to 0.149. Therefore it was concluded that between 11.2% to 14.9% of the variation in Secure Remote Access.

4.7 Discussion of The Results

The study involved 91 respondents from Kericho County staff who were engaged in teleworking. This sample size represents the individuals who were the subjects of the study. A sample size of 91 is a reasonable size for a study and can provide meaningful insights into the factors affecting remote access security. The study focused on six independent variables: Technology, Organizational Factors, Employees, Monitoring & Evaluation, Resource Management & Controls, and Data Protection & Monitoring. These variables were chosen as potential factors influencing remote access security. They were investigated to determine their significance in explaining and predicting the level of remote access security.

The study used a significance level of 5% (often denoted as $\alpha = 0.05$). This significance level is used to assess the statistical significance of the results. In this context, it indicates that the researchers considered a p-value of less than 0.05 as statistically significant. If the p-value associated with a result is less than 0.05, it suggests that the result is unlikely to have occurred by chance. The general objective of the research was to develop a model for safe remote employee access to corporate networks. This objective reflects the practical aim of the study: to create a model or framework that organizations and employees can use to ensure secure remote access to corporate networks. the research study focused on understanding and modeling the factors affecting remote access security in a teleworking context.

The study's sample size, choice of independent variables, significance level, and overall objective suggest a comprehensive approach to addressing the challenges and opportunities associated with remote access security in the context of modern work environments. The results of the study, as discussed in previous sections, indicate that the chosen independent variables collectively have a significant impact on remote access security. This information can be valuable for organizations and policymakers looking to enhance security in the context of teleworking and remote access to corporate networks.

The data collection process revealed that effective management of the technological devices used in teleworking is crucial. This implies that how organizations handle and oversee the devices their employees use for remote work is a critical factor in ensuring security. Managing these devices may involve setting up security protocols, ensuring software updates, and implementing other safeguards to protect corporate data and systems. The information suggests that the study's findings align with those of (Kasinathan et al.,2021) who conducted research. According to (Kasinathan et al., 2021) progressive organizations have incorporated teleworking into their operations, and effective management of devices is a key element in ensuring the proper usage of these devices. This correlation indicates that the research you mentioned is consistent with existing literature on the importance of device management in the context of teleworking.

The information also refers to the work of (Porcius, 2020), who underscores the importance of technological devices in teleworking. Porcius specifically emphasizes the use of VPN (Virtual Private Network) technology and smart devices. VPNs are commonly used for secure remote access to corporate networks, and smart devices can offer increased flexibility and efficiency in remote work. This suggests that the study recognizes the significance of advanced technology and security measures in remote work arrangements.

The study identifies employees as a crucial aspect of teleworking integration. This implies that the behavior, practices, and actions of employees play a significant role in determining the success of remote work arrangements. Their actions and adherence to security protocols can impact information security. These elements, such as monitoring, resource management, and data protection, are mentioned as guiding County employees on how to mitigate information security threats. This highlights the importance of having proper measures, controls, and tools in place to ensure the security of data and systems in a teleworking environment.

The study's findings indicate that organizational factors are integral in achieving remote secure access. These factors likely refer to the organization's policies, procedures, and practices that influence the security of remote access. This finding aligns with research conducted by Haber in 2017, which suggests that organizational factors are closely linked to privacy and security risks. The information also highlights a contrast between the current study's findings and those of (Sarma, 2020). Sarma's research suggested that organizations with younger generation employees are better at remote access security. However, the current study's findings indicate that a security culture related to teleworking can impact remote access security regardless of the age demographic of users.

This discrepancy suggests that other factors, such as organizational culture and practices, may be more influential than the age of employees in determining remote access security. It's worth noting that a significant proportion of the respondents (68.3%) fell within the age range of 25 to 35 years, indicating a youthful population. This demographic information provides context and suggests that the study's findings and conclusions should be considered in light of the age distribution of the respondents.

The additional information expands on the study's findings related to teleworking integration, organizational factors, and the role of employees in remote access security. It also highlights the discrepancy with prior research regarding the influence of employee age on remote access security and emphasizes the role of security culture. This information underscores the multifaceted nature of remote access security and the importance of considering various factors, including organizational practices and employee behaviors, in achieving a secure teleworking environment.

The research published by (Iwaniuk et al. 2009), suggests that technology users, when perceiving a threat, become motivated to overcome and avoid that threat. This research posits that when individuals using technology (in this case, teleworking technology) perceive a threat to their security, they are more likely to take steps to overcome and avoid that threat. In the context of teleworking, this threat could include information security risks or data breaches associated with remote access. The information also highlights the role of employee training and education in enhancing knowledge and practices when using personal devices to access company information technology. This implies that organizations should invest in training and educational programs to equip employees with the skills and awareness needed to use technology securely.

The Technology Threat Avoidance Theory proposes that when technology users perceive security threats, they become motivated to avoid and overcome these threats. This motivation can drive individuals to seek education and training, which, in turn, can enhance their knowledge and practices related to remote access security. Ultimately, this can lead to improved corporate network security, highlighting the importance of security awareness, training, and education in the context of teleworking and technology usage.

The presentation covered the fundamentals of linear regression, including odds, odds ratio, logistic curve, logit transformation, assumption, choosing dependent and independent variables, fitting, reporting, and interpretation. Reading through the literature revealed significant flaws in the reporting and application of the linear regression model. The accuracy of the regression model was questioned in numerous research due to the modest ratio of outcome events to predictor variables (events per variable). Furthermore, most studies did not provide goodness-of-fit metrics, regression diagnostics, or validation analyses. The appropriate application of this potent and intricate modelling technique necessitates great attention to detail in both the model's form specification and the computation and interpretation of the coefficients. We demonstrated how the linear regression ought to be done. It is recommended that researchers be more thorough and pay greater attention to these guidelines concerning the use and reporting of linear regression models. In future, researchers could compare linear regression with other emerging classification algorithms to enable better or more rigorous evaluations of such data.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presented the results of the research conducted on the model of secure remote access to enterprise networks by employees within Kericho County. The findings highlighted the awareness, utilization, benefits, and challenges associated with remote access. The discussion contextualized these findings within the broader scope of existing literature and organizational implications. The chapter further discusses conclusions and recommendations.

5.2 Summary

At the core of this research was the profound objective to comprehensively assess the security posture of teleworking enterprise networks within the geographical domain of Kericho County. The lens of inquiry was specifically focused on understanding and analyzing the behaviors of employees concerning technology utilization, adherence to organizational policies, and the overall teleworking environment. These behavioral aspects were recognized as critical variables that could significantly impact the information security landscape within this region.

The geographical context of Kericho County provided an insightful backdrop for this study, allowing for a more localized analysis of teleworking dynamics. Kericho County stood as a microcosm, illustrating the broader trend of teleworking adoption. The research aimed to probe into this trend and unravel the associated security implications. A pivotal revelation of this research was the notable embrace of teleworking among employees within Kericho County.

The data indicated a substantial number of employees who had transitioned into teleworking. This finding holds immense significance, shedding light on the changing work

culture and practices within the region. Teleworking had emerged as a viable and prevalent mode of work, a shift that has been further accelerated by various socio-economic factors and, most prominently, the global COVID-19 pandemic. Additionally, the study keenly observed and documented the mechanisms put in place by the organization in Kericho County to facilitate teleworking. These mechanisms encompassed a spectrum of strategies and tools designed to enable a smooth transition to teleworking. They included provisions for secure remote access, technological infrastructures, and policy frameworks.

Understanding and analyzing these mechanisms was vital in comprehending the support system that the organization had established to ensure a seamless teleworking experience for its employees. To grasp the nuances of information security within this teleworking paradigm, it was essential to scrutinize how employees interacted with technology.

The research delved into the intricate relationship between employees and technology in the teleworking context. This involved evaluating the proficiency of employees in utilizing digital tools, their adherence to security protocols, and their comprehension of potential security threats associated with teleworking. Furthermore, organizational policies emerged as a critical facet of the study. Policies serve as guiding principles, delineating the framework within which employees operate. This study sought to understand the extent to which employees within Kericho County adhered to these policies in the teleworking milieu. It aimed to gauge the awareness levels and compliance rates concerning information security policies. Understanding this aspect was imperative, as policy adherence is directly intertwined with the overall security posture of the enterprise network.

The teleworking environment itself was another crucial element under scrutiny. The study recognized the diverse teleworking setups and conditions within Kericho County. It investigated the range of environments in which teleworking was being practiced, ranging from

home offices to public spaces. Understanding the nuances of these teleworking environments was essential in evaluating the associated security risks and formulating targeted security strategies.

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 Kericho county 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 enjoying a home office, there were also 38.4% of staff who lived with people that work in the county.

5.3 Conclusion

The landscape of modern work is rapidly evolving, with remote work becoming increasingly prevalent, particularly in the enterprise networks in all the organizations. The COVID-19 pandemic accelerated this shift, compelling organizations to adopt teleworking as

a fundamental component of their operational model. While remote work offers flexibility and operational continuity, it also introduces significant information security challenges. Understanding and addressing these challenges are of paramount importance to safeguard sensitive information and maintain the integrity of operations.

The primary objective of this research was to identify and delve into the factors that influence information security within the realm of teleworking. This focus emerged as a critical concern given the growing prevalence of remote work in the enterprise sector in all organizations. The advent of teleworking, while beneficial, also raises crucial questions about how to protect sensitive information in an environment that extends beyond the traditional office space. This research serves as an essential guide for organizations navigating the complex terrain of information security in the context of teleworking. To provide a deeper understanding, the study examined key factors and challenges that impact information security in teleworking. Let's explore these in greater detail. One of the significant findings of this research was the heightened risk of industrial espionage when employees work from home, particularly in environments that lack adequate security measures. This risk is further exacerbated when employees share their teleworking space with individuals from the same sector. In such scenarios, sensitive corporate information becomes susceptible to unauthorized access, raising the specter of data breaches and security lapses.

The implication here is clear: secure home offices and isolated workspaces are essential prerequisites for employees engaged in teleworking as discussed by (Bourne, 2022). This underscores the importance of creating an environment where employees can work without the risk of industrial espionage. For organizations, this entails providing guidelines for creating secure home offices and ensuring that employees understand the significance of maintaining a secure workspace.

The study emphasizes the necessity for organizations to establish, communicate, and enforce clear information security policies specifically designed for teleworking. An information security policy that is well-understood by employees is a fundamental component in ensuring that security protocols and best practices are followed when working remotely. An effective information security policy outlines the dos and don'ts of handling sensitive information. It also covers secure communication protocols, encryption standards, and the protection of access credentials. When employees are aware of these guidelines and the importance of adhering to them, the risk of security breaches is significantly reduced.

Clear communication and training about these policies are vital to safeguard the integrity and confidentiality of shared information. The research underscores the need for organizations to invest in and provide the requisite infrastructure to support teleworking effectively. This infrastructure includes secure virtual private network (VPN) connections, robust access controls, and encryption tools. Ensuring that employees have access to a secure teleworking environment is vital for maintaining information security. Secure VPN connections are particularly crucial as they enable employees to access corporate resources securely from remote locations. Access controls ensure that only authorized personnel can access sensitive information, reducing the risk of unauthorized data breaches. Encryption tools add an extra layer of security by safeguarding data during transmission, even in potentially insecure network environments.

The findings of this research extend beyond its immediate context and hold broad relevance for organizations in the enterprise sector and financial institutions. As teleworking continues to be a prevalent mode of work, the identified risks and recommendations can guide these organizations in their efforts to maintain robust information security in the remote work setting. By addressing factors like industrial espionage risks, implementing clear information security policies, and providing the necessary infrastructure, organizations can effectively

mitigate security threats and protect their sensitive information. In doing so, they ensure the resilience and security of their operations, even in an environment where remote work has become the new norm.

The research represents a critical step in understanding and addressing the multifaceted challenges of information security in teleworking. By recognizing these challenges and implementing the recommended solutions, organizations can navigate the complex landscape of remote work with confidence, ensuring that their sensitive information remains protected and their operations continue to thrive in the digital age.

In conclusion, our project, "A Linear Regression Model of Secure Remote Access to Enterprise Networks By Employees: A Case Study Of Kericho County," provides valuable insights into the intricacies of secure remote access within enterprise networks and contributes significantly to the field of data communication. Through a rigorous examination of factors influencing remote access security, including authentication mechanisms, encryption protocols, network configurations, and user behavior patterns, we have developed a novel linear regression model. This model serves as a powerful tool for analyzing and optimizing the performance of secure remote access protocols, offering organizations a means to enhance their network security posture effectively. By conducting a detailed case study in Kericho County, we have demonstrated the real-world applicability of our methodology and findings, providing actionable recommendations for improving remote access security practices in similar organizational settings. Our research underscores the importance of proactive security measures in safeguarding enterprise networks against emerging threats and vulnerabilities.

Furthermore, our study emphasizes the need for continuous innovation and adaptation in the realm of data communication, particularly concerning secure remote access protocols. As organizations increasingly rely on remote access to facilitate operations and collaboration,

the significance of robust security measures cannot be overstated. In essence, our project highlights the potential of data-driven approaches, such as linear regression modeling, to address complex challenges in network security and data communication. By offering practical insights and solutions, we aim to empower organizations to strengthen their remote access security posture and mitigate risks effectively in an ever-evolving threat landscape. Moving forward, we advocate for ongoing research and collaboration to advance the field of data communication and ensure the resilience of enterprise networks in an increasingly interconnected world.

5.4 Contributions of the study

In the contemporary landscape of corporate enterprise networks, the utilization of Remote Access Security has gained pronounced prominence. This surge in importance can be attributed to the extensive digitization of organizational operations, where nearly every facet of business has migrated to digital platforms. As a result, employees increasingly rely on their personal devices to access critical company information. The conveniences of this approach are evident; however, they come with the significant responsibility of ensuring that remote access remains secure and impervious to external threats.

The study is a notable contribution to the ever-evolving discourse on secure remote access. It enriches the pool of knowledge by shedding light on the practical implementation of Secure Remote Access as a Usable Endpoint Security System, a concept proposed by (Powell, 2021). This system operates unobtrusively in the background, vigilantly monitoring the diverse devices within the organizations for remote access security. By studying and implementing such advanced security measures, the research underlines the pressing need for an improved model to bolster remote access security. One such exemplar is the teleworking, which aligns with the broader objective of safeguarding remote access.

The study recognizes the significance of employing such programs to ensure that the company's information remains confidential, intact, and invulnerable to external threats. This underscores the urgency of gathering insights and knowledge on how best to institute and uphold remote access security policies effectively.

The sentiments and perspectives gathered by this research predominantly emanate from junior employees, who constitute the most populous demographic within Kericho County. This demographic specificity is consequential, as it provides valuable insights into the attitudes, practices, and expectations of the next generation of the workforce. Their perspective is often informed by digital nativism, a fluency in technology, and an inherent familiarity with remote work and the use of personal devices for professional purposes. This knowledge, acquired through rigorous research and observation, will be instrumental in empowering top management to make well-informed decisions regarding the utilization of remote access security within their organizations. The study brings forth a wealth of data, trends, and insights that can guide executive decisions and influence corporate strategies. It fosters a profound understanding of the expectations.

Overall, our study not only addresses the specific challenges of secure remote access within enterprise networks but also contributes to the broader understanding of data communication by offering insights, methodologies, and solutions applicable to various organizational contexts. Through our research, we aim to foster innovation and progress in the field of data communication, ultimately enhancing the security and efficiency of remote access protocols for organizations worldwide.

5.5 Recommendations

The resilient work environment in an era where remote work is becoming increasingly prevalent. Delving into the realm of organizational considerations for information security and

remote work, there are critical facets that merit comprehensive exploration. The study advocates for a meticulous focus on the 17.9% of employees who have not received any information security training. This subset represents a potential vulnerability that needs immediate attention. Information security, being a highly dynamic and ever-evolving field, necessitates ongoing training and regular policy reviews to keep employees abreast of the latest threats, best practices, and protocols.

Securing the information accessed, processed, and stored at teleworking sites is of paramount importance. This encompasses not only the digital realm but extends to the physical security of teleworking locations. Communication security in remote access protocols is a pivotal consideration, advocating for the enforcement of secure protocols such as VPN. Furthermore, assessing the sensitivity of transmitted information is crucial, reinforcing the need for stringent security measures to preserve data integrity and confidentiality.

Restricting access to systems for teleworking personnel is a prudent measure. Access should be tailored to precisely the resources required for their day-to-day activities. Adopting a principle of least privilege ensures that access is not left open-ended but granted on a need-only basis, thereby reducing the risk of unauthorized access. Employing vigilant monitoring to detect any anomalous behavior is a proactive strategy, reinforcing security measures and thwarting potential threats.

Addressing practical challenges, supporting employees in acquiring cost-efficient power backup solutions amplifies their ability to maintain uninterrupted work sessions while telecommuting. This demonstrates organizational commitment to ensuring a conducive remote work environment, bolstering productivity and preparedness for unforeseen disruptions.

Teleworking can indeed serve as a crucial staff backup plan, embodying a robust business continuity strategy. In times of calamity that may incapacitate a physical workplace,

employees working remotely can function as a resilient contingency, ensuring operational continuity even amidst adversity.

Looking ahead, the incorporation of advanced technologies, particularly security software leveraging biometric identification, can significantly enhance remote work security. Biometric identification provides a robust layer of authentication, adding an extra dimension of assurance in verifying the identity of remote employees. As technology advances, further development in this domain will optimize security protocols for employees operating from diverse locations.

The organization's dedication to fortifying information security in the realm of remote work is not only a prudent business strategy but a commitment to safeguarding sensitive data and ensuring seamless operations. The recommendations and considerations outlined serve as a roadmap towards a secure, adaptive, and effective secure remote access.

5.6 Limitation of the Study

Exploring the realm of information security is undoubtedly a sensitive endeavor, one that often navigates through a web of complexities and apprehensions. The study delved into this sensitive territory, and throughout the process, there were noteworthy observations and challenges encountered. One of the most prominent challenges was the general hesitance and reluctance exhibited by the respondents. Their concerns primarily revolved around the fear that the information they shared might be used against them. This apprehension could be attributed to the heightened awareness and scrutiny surrounding data privacy and security issues in the modern era.

Respondents, understandably cautious, seemed to question the intent and source of the questionnaire. It's noteworthy that despite advance communication from the researcher, some respondents felt compelled to verify the source multiple times before participating. The

skepticism exhibited by some respondents also reflects the prevalent concern about cybersecurity. The era of cyber threats and data breaches has made individuals increasingly vigilant about sharing information, especially when they perceive a potential risk to their personal or professional security (Powell, 2021). The fear of malicious intent from unknown sources is a sentiment that can be common in today's interconnected world.

Furthermore, it's important to recognize that some aspects of information security are inherently delicate and, therefore, challenging to address openly in a questionnaire format. Certain nuances of security practices and protocols might be closely guarded for valid reasons, making it difficult for respondents to share this information comprehensively. The study also encountered issues related to the respondents' level of knowledge and exposure in the field of information security. It was apparent that not all participants had a deep or comprehensive understanding of the technical jargon and intricacies associated with this domain. This lack of exposure and familiarity with the subject matter posed a challenge in obtaining accurate and detailed responses.

The study on information security navigated through a landscape marked by sensitivity, skepticism, and varying levels of expertise among respondents. These observations underscore the critical importance of trust-building, clarity, and respect for privacy when conducting research in this field. The challenges encountered provide insights into the evolving dynamics of information security and the need for well-informed and ethically sensitive research practices in this domain.

REFERENCES

Aldawood, H, & G. Skinner, (2019). "*An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions*," in 2019 the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia 2019

Alhassan, MA & Adjei, A.Q. (2017). Information security in an organization.*International Journal of Computer*, 14 (1), 100-116.

Avorgbedor, F., & Liu, J. (2020, July). Enhancing User Privacy Protection by Enforcing Clark-Wilson Security Model on Facebook. In *2020 IEEE International Conference on Electro Information Technology (EIT)* (pp. 155-161). IEEE.

Bada, M., A.M. Sasse, & J.R. Nurse, (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprintarXiv*:1901.02672.

Bagaskara, A. I., Hilmiana, H., & Kamal, I. (2021). Influence of Flexible Work Arrangement and Work Environment on Employee Performance Through Work-Life Balance During The Covid-19 Pandemic. *AFEBI Management and Business Review*, *6*(1), 73-85.

Belal, S. M., & Rahman, M. D. (2021, December). Covid Best Practices for Cyber Risk Management. In *Abu Dhabi International Petroleum Exhibition & Conference*. OnePetro.

Béland, L. P., Brodeur, A., & Wright, T. (2020). "*The short-term economic consequences of Covid-19: exposure to disease, remote work and government response*," in IZA Institute of labor economics Discussion Papers, No. 13159, (Bonn: IZA Institute of labor economics).

Belzunegui-Eraso, A., &Erro-Garcés, A. (2020). Teleworking in the Context of the Covid-19 Crisis. *Sustainability,* 12(9), 3662.

Bergvall, R. (2021). Secure remote access to a work environment.

Bett, F., Sang, H., &Chepkwony, P. (2022). Flexible Work Arrangement and Employee Performance: An Evidence of Work-life Balance Practices. *East African Journal of Business and Economics*, *5*(1), 80-89.

Bourne, J. (2022). Technology: Securely managing remote working and distributed workflows. *Inside Film: If*, (204), 50-51.

BrighterMonday, (2019). Millennials and the Digital Market Place. How to keep Millennials Productive in the Workplace.

Burnik, U., Dobravec, Š., &Meža, M. (2019). Design of a secure remote management module for a software-operated medical device. *Biomedical Engineering/Biomedizinische Technik*, *64*(1), 67-80.

Campbell, M. (2020). Beyond zero trust: trust is a vulnerability. *Computer*, *53*(10), 110-113.

Chung, H. (2018). *Future of Work and Flexible Working in Estonia: The Case of Employee-Friendly Flexibility;*ArenguseireKeskus: Tallinn, Estonia. Available online: http://www.wafproject.org

Clarke, N. (2021). Cyber Attack: Past, Present, and Future. Apress.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

CSS, (2022). Computer Systems Security - CSS- ReShare System - File Sharing System Through a Web Application Portal - Scientific Figure on ResearchGate.Available from:https://www.researchgate.net/figure/Clark-Wilson-Model-Ravi-Sandhu_fig1_326367566[accessed 18 Feb, 2022]

Dannels, S. A. (2018). Research design. In *The reviewer's guide to quantitative methods in the social sciences* (pp. 402-416). Routledge.

Flanigan, J. (2018). Zero Trust Network Model. *Tufts University: Medford, MA, USA*.

Haber, M. J. (2020). Remote Access. In *Privileged Attack Vectors* (pp. 239-250). Apress, Berkeley, CA.

Iordache, A. M. M., Dura, C. C., Coculescu, C., Isac, C., &Preda, A. (2021). Using Neural Networks in Order to Analyze Telework Adaptability across the European Union Countries: A Case Study of the Most Relevant Scenarios to Occur in Romania. *International Journal of Environmental Research and Public Health*, *18*(20), 10586.

Iwaniuk, A., Hawrysz, L., Bulińska-Stangrecka, H., &Huras, P. (2021). Barriers to the effectiveness of teleworking in public administration. *ZeszytyNaukowe. OrganizacjaiZarządzanie/PolitechnikaŚląska*.

Janczewski, L., & Colarik, A. M. (2020). Cyber Warfare and Cyber Terrorism. IGI Global.

Kalakuntla, Rohit, Vanamala, AnveshBabu&Kolipyaka, Ranjith Reddy, (2019). "Cyber Security" HOLISTICA – Journal of Business and Public Administration, vol.10, no.2, 2019, pp.115-128. https://doi.org/10.2478/hjbpa-2019-0020

Kasinathan, P., Martintoni, D., Hofmann, B., Senni, V., &Wimmer, M. (2021, December). Secure Remote Maintenance via Workflow-Driven Security Framework. In *2021 IEEE International Conference on Blockchain (Blockchain)* (pp. 29-37). IEEE.

Kim, D., & Solomon, M. (2018). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

Langat, E. K. EFFECT OF DATA SECURITY ON IMPLEMENTATION OF ELECTRONIC PROCUREMENT IN COUNTY GOVERNMENT OF KERICHO, KENYA.

Linneberg, M. S., &Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative research journal*.

McKay J, Marshall P, &Hirschheim R. (2021). The Design Construct in Information Systems Design Science. *Journal of Information Technology*, 27(2):125-139.

Montagut, W.V.; Carrillo, L.P.V. & Delgado, M.D.P.S. (2017). Model for implementation of teleworking in software development organizations. *Sistem as Telemática*, 15, 29–44.

Porcius, I. (2021). The Rise of Telework and The Struggle Towards Cyber Security. *Fiat Iustitia*, *1*(1), 148-157.

Powell, C. R. (2021). The Impact of Telework on Organizational Cybersecurity during the COVID-19 Pandemic (Doctoral dissertation, Utica College).

Sarma, C. (2022). Secure Remote Workplace 4EM Model. In *Advances on Smart and Soft Computing* (pp. 367-377). Springer, Singapore.

Schlehahn, E. (2020). Cybersecurity and the State. *The Ethics of Cybersecurity*, 205.

Scott, J. J. (2019). Learn to use Cronbach's coefficient alpha test in R with data from theBritish Crime Survey (Unrestricted Teaching Dataset) (2007--08).

Seemma, P.S., NandhiniM,&Sowmiya. (2018). Overview of Cyber Security. IJARCCE. 7. 125-128. 10.17148/IJARCCE.2018.71127.

Srinivas, J., A.K. Das, & N. Kumar, (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92: p. 178-188.

Stafford, V. A. (2020). Zero trust architecture. *NIST Special Publication*, *800*, 207.

Türkeș, M. C., &Vuță, D. R. (2022). Telework: Before and after COVID-19. *Encyclopedia*, *2*(3), 1370-1383.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.

Zeng, K., & Li, Z. (2020). Best Practices in Cybersecurity for Utilities: Secure Remote Access.

APPENDIX I

Data Collection Letter

Thika Road, Ruaraka
P.O. Box 56808-00200 Nairobi Kenya
Pilot Line: +254 20 8070408/9

Tel: +254 20 3537842
Fax: +254 20 8561077
Mobile: +254 734 888022, 710 888022
Email: kcau@kca.ac.ke
Website: www.kca.ac.ke

BOARD OF POSTGRADUATE STUDIES

KCAU/BPS/Sept. 23/1 27th September 2023

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

RE: KETER KIPKEMOI EDWIN REG NO: 18/03647

It is my distinct pleasure to introduce to you Edwin Keter who is a student in our institution pursuing a Master of Science in Data Communications in the School of Technology.

Edwin is conducting a research on a topic titled: "*A Model of Secure Remote Access to Enterprise Networks by Employees: A Case Study of Kericho County* which is part of the requirements of the program he is pursuing. The research as well as the data procured thereof shall be used for academic purposes only.

Any assistance accorded to him is highly appreciated.

In case of further inquiry, do not hesitate to contact the undersigned.

Yours faithfully,

Dr. Jackson Ndolo
Director, Board of Post Graduate Studies

APPENDIX II

Questionnaire

This questionnaire is designed to collect data for a study assessing factors affecting information security in data teleworking. Your participation in this research is highly appreciated. You are kindly requested to complete the questionnaire honestly. The information provided will be used strictly for academic purposes and will be treated with the highest level of confidentiality.

Section 1: Demographic Data

1. What is your position or title in the organization?
2. How long have you worked with Kericho County?
   Less than 5 years
   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 1–5.
   1 Not at all [ ]
   2 Small extent [ ]
   3 Moderate extent [ ]
   4 Great extent [ ]
   5 Very great extent [ ]
4. To what extent have you undertaken training on information security related to teleworking?
   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?
   1 Not at all [ ]
   2 Small extent [ ]
   3 Moderate extent [ ]
   4 Great extent [ ]
   5 Very great extent [ ]
6. To what extent do the people you interact with during teleworking also work in the SACCO?
   1 Not at all [ ]
   2 Small extent [ ]
   3 Moderate extent [ ]
   4 Great extent [ ]
   5 Very great extent [ ]

Section 3: Levels of Risk Exposure (Technology-Related)

7. What is your source of internet when teleworking?
   [ ] Private Wi-Fi
   [ ] Public Wi-Fi
   [ ] Phone tethering
   [ ] Cyber café
8. Is your laptop hard disk encrypted?
   [ ] Yes
   [ ] No
9. Which credentials do you use to connect remotely?
   [ ] Domain credentials
   [ ] Local credentials
10. Have you ever lost your mobile device (e.g., laptop) while teleworking?
    [ ] Yes
    [ ] No
11. Are you allowed to move data between devices using removable devices (e.g., flash disks)?
    [ ] Yes
    [ ] No
12. Have you ever lost data through loss of a laptop or removable device?
    [ ] Yes
    [ ] No
13. Has any of your devices been affected by malware while working remotely?
    [ ] Yes
    [ ] No
14. Do you ever work using personal devices (e.g., personal laptops) when teleworking?
    [ ] Yes
    [ ] No
15. How do you connect to the office network while working remotely?
    [ ] Applications only require internet
    [ ] Using VPN
    [ ] Other (Specify)
16. How do you communicate with colleagues in the office?
    [ ] Phone calls
    [ ] Skype
    [ ] MS Teams
    [ ] GTalk

Section 4: Levels of Risk Exposure (Organizational-Related)

17. To what extent do you think the County supports teleworking?
    1 Not at all [ ]
    2 Small extent [ ]
    3 Moderate extent [ ]
    4 Great extent [ ]
    5 Very great extent [ ]
18. How often do you telework?
    [ ] Every day of the week
    [ ] Twice a week
    [ ] Weekly
    [ ] Biweekly

[ ] Monthly
[ ] Rarely
[ ] Never

19. What kind of access do you have on the systems when working remotely?
    [ ] Weekday working hours (8 a.m. – 5 p.m.)
    [ ] Full-time access (24/7)
    [ ] Access on request and as required
20. Do you understand the information security policy?
    [ ] Yes
    [ ] No
21. Have you read the information security policy document?
    [ ] Yes
    [ ] No
22. Do you understand the consequences of non-compliance with the information security policy?
    [ ] Yes
    [ ] No

Section 5: Levels of Risk Exposure (Environment-Related)

23. To what extent do you face power outages while teleworking?
    1 Not at all [ ]
    2 Small extent [ ]
    3 Moderate extent [ ]
    4 Great extent [ ]
    5 Very great extent [ ]
24. Do you have a power backup in case power is interrupted?
    [ ] Yes
    [ ] No
25. To what extent do you face internet outages while teleworking?
    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

Section 6: Network and Security Administration Staff Only

27. Are you able to tell who is connected remotely at any one time?
    [ ] Yes
    [ ] No
28. Do you give users restricted access to systems?
    [ ] Yes
    [ ] No
29. Are you able to tell the activities being carried out by people connected remotely?
    [ ] Yes
    [ ] No

30. How often is the information security policy updated?