

AFRICA UNIVERSITY

(A United Methodist-Related Institution)

**THE EFFECTS OF REMOTE WORKER ON CYBERSECURITY IN
THE TELECOMMUNICATIONS INDUSTRY**

BY

WIMBAYI P CHIDZVETE (221010)

**A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF EXECUTIVE MASTER'S IN BUSINESS
ADMINSTRATION IN THE FACULTY OF BUSINESS, PEACE, LEADERSHIP
AND GOVERNANCE**

2024

Abstract

In the contemporary digital era, cybersecurity stands at the forefront of organizational concerns, heightened by an increasing wave of cyber threats. This study is set against the backdrop of cybersecurity's escalating importance, especially considering the shift towards remote work prompted by the COVID-19 pandemic. Its core objective is to examine the cybersecurity implications of remote work within the telecommunications sector, aiming to unearth vulnerabilities, threats, and devise effective countermeasures. Such insights are intended to empower industry stakeholders, policymakers, and cybersecurity experts to preemptively tackle the challenges associated with securing remote work environments. Employing a survey questionnaire for data collection and utilizing descriptive statistics for the analysis of quantitative data, this research engaged a cohort of 278 participants, successfully garnering responses from 230 individuals, which translates to an impressive response rate of 82.7%. The findings culminate in pragmatic recommendations for the telecommunications industry, advocating for heightened cybersecurity protocols, comprehensive remote work policies, and increased investments in technological infrastructure and staff training. It's important to note, however, that the study's primary limitation lies in its focus on a singular entity within the telecommunications field, which may limit the direct applicability of its findings across different organizations, given the variance in organizational cultures and policies. Despite this, the research significantly advances the discourse on remote work cybersecurity, laying a solid foundation for future inquiries and equipping stakeholders with a basis for proactive measures against emerging cyber threats and vulnerabilities.

Key Words for the Research

Remote worker,

Remote working,

Cybersecurity,

Telecommunications industry,

Effects

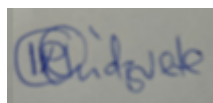
Declaration Page

I, Wimbayi P Chidzvete declare that this dissertation is my original work except where sources have been cited and acknowledged. The work has never been submitted, nor will it ever be submitted to another university for the award of a degree.

Student's Full Name

Student's Signature (Date)

Wimbayi P Chidzvete



10/04/2024

Main Supervisor's Full Name

Main Supervisor's Signature (Date)

AGRIPAH KANDIERO (PhD)



13/04/2024

Copyright Page

No part of the dissertation/thesis may be reproduced, stored in any retrieval system, or transmitted in any form or by any means for scholarly purposes without prior written permission of the author or of Africa University on behalf of the author.

Acknowledgements

I would like to express my deepest gratitude to God Almighty for His guidance, blessings, and protection throughout my academic journey. Without His grace and wisdom, this dissertation would not have been possible. I am humbled by His boundless love and grateful for the strength He has provided me during challenging times.

I would like to express my deepest appreciation and gratitude to my advisor, Dr. Agripah Kandiero. Your guidance, expertise, and unwavering support throughout the entire research process have been invaluable. Your insightful feedback pushed me to grow academically.

I would also like to express my gratitude to my classmates EMBA Class Aug2022 your support and encouragement together with your valuable discussions helped me sail through. Your camaraderie and shared experiences have made the challenges more manageable and the successes more fulfilling.

To my friends, family and colleagues with special mentioning going to Vincent Mutimbanyoka and Jessy Chisale, thank you for walking with me throughout this academic journey. I will forever be indebted to you.

I would like to extend my thanks to the participants of this study, whose willingness to share their experiences and insights made this research possible. Your contributions have been invaluable, and I am deeply grateful for your time and cooperation.

Although it is impossible to name everyone who has contributed to this dissertation, please know that your support, in whatever capacity, is deeply appreciated. Thank you all for being a part of this journey and for helping me achieve this milestone.

Dedication

I would also like to express my heartfelt gratitude to my husband Kiven Mutimbanyoka, whose unconditional love, encouragement, and sacrifices have made it possible for me to pursue my educational goals. Your endless support and belief in my abilities have been my driving force, and I dedicate this dissertation to you with immense appreciation and love.

List of Acronyms and Abbreviations

| | |
|-----|------------------------------|
| IT | Information Technology |
| HR | Human Resources |
| PMT | Protection Motivation Theory |
| VPN | Virtual Private Network |

Table of Contents

| | |
|--|------|
| Abstract | iii |
| Key Words for the Research | iii |
| Declaration Page | iv |
| Copyright Page..... | v |
| Acknowledgements..... | vi |
| Dedication | vii |
| List of Acronyms and Abbreviations | viii |
| APPENDIX..... | xi |
| CHAPTER 1 INTRODUCTION | 1 |
| 1.1 Introduction..... | 1 |
| 1.2 Background to the study | 2 |
| 1.3 Statement of the problem | 4 |
| 1.4 Research Objectives..... | 5 |
| 1.5 Research Questions | 5 |
| 1.6 Assumptions/ Hypotheses | 5 |
| 1.7 Significance of the study..... | 7 |
| 1.8 Delimitation of the study | 10 |
| 1.9 Limitation of the study | 11 |
| CHAPTER 2 REVIEW OF RELATED LITERATURE..... | 14 |
| 2.1 Introduction..... | 14 |
| 2.2 Theoretical framework..... | 22 |
| 2.3 Relevance of the theoretical frame to the study | 25 |
| 2.4 Summary | 35 |
| CHAPTER 3 METHODOLOGY | 37 |
| 3.1 Introduction..... | 37 |
| 3.1.1 Quantitative Research | 37 |
| 3.2 The research design..... | 39 |
| 3.3 Population and Sampling | 41 |
| 3.4 Data collection instruments..... | 42 |
| 3.5 Analysis and organization of data..... | 45 |
| 3.6 Ethical Consideration..... | 46 |
| 3.7 Summary | 49 |
| CHAPTER 4: DATA PRESENTATION, ANALYSIS, AND INTERPRETATION | 51 |

| | |
|--|----|
| 4.1 Introduction..... | 51 |
| 4.2 Data presentation and analysis..... | 51 |
| 4.2.2 Findings on Remote Work and Cybersecurity | 54 |
| 4.2.3 Findings on Cybersecurity Measures..... | 57 |
| 4.2.4 Employee Awareness and Training | 59 |
| 4.2.5 Key Technological Solutions..... | 62 |
| 4.2.6 Regulatory and Compliance Landscape..... | 65 |
| 4.3 Discussion and interpretation..... | 69 |
| 4.4 Discussion of Results..... | 73 |
| CHAPTER 5: SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS | 75 |
| 5.1 Introduction..... | 75 |
| 5.2 Summary Discussion of Findings | 75 |
| 5.4 Implications..... | 76 |
| 5.5 Conclusions..... | 77 |
| 5.6 Recommendations..... | 80 |
| 5.7 Suggestions for further research | 85 |
| REFERENCES | 88 |
| APPENDIX 1: Questionnaire Survey Instrument..... | 92 |
| SURVEY QUESTIONNAIRE LINK :..... | 96 |
| APPENDIX II: AUREC Approval letter | 97 |

APPENDIX

| | |
|--|----|
| APPENDIX 1: Questionnaire Survey Instrument..... | 71 |
| SURVEY QUESTIONNAIRE LINK..... | 75 |
| APPENDIX II: AUREC Aproval letter..... | 76 |

CHAPTER 1 INTRODUCTION

1.1 Introduction

Remote workers have been embraced by many organisations especially those in telecommunications and technology industries as a business continuity strategy during Covid 19 in Zimbabwe. However, little is yet known about some of the more fundamental consequences of remote workers, including its effects on cyber security compared to working from the office (WSJ, 2020; Financial Times, 2021). The Covid-19 pandemic accelerated the process of remote working by forcing a large fraction of the global workforce to switch to working from home at least temporarily. During the COVID-19 pandemic, a significant increase in the number of employers who offer employees the possibility to work remotely has also been facilitated by national approaches to improving the epidemiological situation, which prescribed remote work for all whose work specifics allow it. At the same time, cyber threats have increased during the pandemic, which highlights the need to adjust the approaches of employers to cyber-risk management, (Assata, L et al,2022).

This dissertation explores the adoption of remote workers in Zimbabwean telecommunications industry. It aims to analyse the effects of remote worker on cyber security to develop a model that can be used to improve cyber security when working remotely.

The research was conducted using a quantitative approach. The primary data collection instrument used was the survey questionnaires and data analysis were carried out using regression analysis and structural equation modelling. The study's findings make a

significant contribution to the existing body of knowledge on the cyber security risks associated with remote workers.

1.2 Background to the study

According to Eurofound (2020), approximately 40% of employees in the EU began to telework full-time due to the pandemic. In the EU, teleworkers were approximately 5% of all employees in 2000, and before the outbreak, just 15% of the employed in the EU had ever worked from home. While remote working (or work from home) was not introduced because of the pandemic, the healthcare emergency pushed enormously towards this shift. Therefore, adopting new forms of work organization based on flexibility and autonomy of the employees in terms of the places and times of work was a strategic need for organizations facing Covid, Bruna Ferrara et al (2021).

The Fourth Industrial Revolution is being driven and inspired by technology daily. The nature of employment, employee interactions, and employee experiences in organisations altered because of digital technologies. The digital technologies are rapidly improving and allowing people to work from anywhere. Work is no longer a place where people go but what people do. Working from home is still a new concept for most organisations especially in the third world countries and there are very few researches that have been done on this issue, The purpose of this research is to expand on the existing body of knowledge and extend the knowledge to Third world countries and validate to see if remote workers can be used as a permanent solution or can only be used as a contingent measure for business continuity during crisis situations.

Most studies on the effects of remote workers have been conducted During the Covid-19 period when most people have been working from home and very few have been

conducted after the Covid-19 pandemic threat. It must be realised that the issues surrounding the effects of remote workers on cyber security during the pandemic and after the pandemic might be different.

Given the changes in the availability of remote workers because of the Covid-19 pandemic, most authors have focused on the cyber risks and challenges posed by changing the daily and work organization habits of remote workers, as well as the use and popularity of the most common types of risk management (security controls). The study focused on employee habits and behaviours as the link in cybersecurity. When working remotely, the protection of work information is important as well as the protection of personal information. The study will analyse the cybersecurity risks associated with changing employee habits in the transition to remote work during the Covid-19 pandemic.

Working from home is still a new concept for most organisations especially in the third world countries and there are very few research that have been done on its effects on cyber security, so this study will be conducted to expand on the existing body of knowledge and compare the findings to those found in other countries to the Zimbabwean experience.

This research is meant to analyse the cyber risks and challenges raised by the Covid-19 pandemic and extended use of remote workers, as well as risk management approaches or controls introduced. The research aims to analyse cybersecurity risks and challenges for telecommunication organizations associated with changing employee habits while working remotely during the Covid-19 pandemic.

The purpose of the study is to establish the various cyber risks associated with remote workers and recommend sustainable cyber-risk management systems to be adopted by remote employees to minimise the risk. To see if remote working can be recommended for telecommunications companies even after Covid-19 or to be used as a contingent measure only .and recommend working from the office due to the cyber risk involved.

1.3 Statement of the problem

The COVID-19 pandemic has ushered in a paradigm shift towards remote work, significantly altering the cybersecurity landscape for companies worldwide. This transition, while enabling flexibility and productivity, has simultaneously introduced complex cybersecurity challenges. Companies, particularly within the telecommunications sector, are now grappling with the integration of remote workers into their operations, exposing them to new vulnerabilities that stem from changes in workforce habits, digital skills, and awareness of cyber hygiene. This shift necessitates a reevaluation and adaptation of organizational cyber-risk management practices to mitigate these emerging risks effectively.

Addressing this gap, the present study aims to explore the multifaceted impact of remote workers on cybersecurity within the telecommunications industry. By identifying specific vulnerabilities and assessing the effectiveness of current cybersecurity measures in the face of remote worker arrangements, this research seeks to provide actionable insights. These insights will be crucial for telecommunication companies as they strive to enhance their cybersecurity frameworks, develop comprehensive policies, and implement targeted training programs and technological solutions. The goal is to secure their networks and systems against potential cyber threats, ensuring operational integrity and safeguarding sensitive information in an increasingly remote work-dominated landscape.

In doing so, this study endeavors to shed light on the pressing cybersecurity challenges posed by remote workers and propose strategies to bolster the resilience of the telecommunications sector against these threats. The focus on the telecommunications industry is particularly pertinent given its critical role in maintaining secure and reliable communication channels—a cornerstone of modern society that becomes even more crucial as remote work practices continue to evolve and expand.

1.4 Research Objectives

1.4.1 Identify and assess the specific cybersecurity vulnerabilities introduced by remote workers within the telecommunications industry.

1.4.2 Evaluate the effectiveness of existing cybersecurity measures in mitigating the risks introduced by remote workers in the telecommunications industry.

1.4.3 Analyse emerging threats and attack vectors associated with remote workers in the telecommunications industry.

1.4.4 Propose strategies and recommendations to enhance cybersecurity resilience in the context of remote workers within the telecommunications industry.

1.5 Research Questions

1.5.1 What are the specific cybersecurity vulnerabilities introduced by remote workers within the telecommunications industry, and how do they impact the overall security posture?

1.5.2 How does the adoption of remote worker practices affect the effectiveness of existing cybersecurity measures in the telecommunications industry?

1.5.3 What are the emerging threats and attack vectors associated with remote workers in the telecommunications industry, and how can organizations mitigate them effectively?

1.5.4 How can organizations within the telecommunications industry enhance their cybersecurity resilience in the context of remote workers?

1.6 Assumptions/ Hypotheses

H0: The introduction of remote workers in the telecommunications industry does not have a significant impact on cyber security vulnerabilities and risks, and there is no notable increase in the number and severity of cyber-attacks.

H1: The introduction of remote workers in the telecommunications industry has a significant impact on cyber security vulnerabilities and risks, resulting in an increase in the number and severity of cyber-attacks.

This hypothesis suggests that the adoption of remote workers in the telecommunications industry introduces new challenges and threats to cyber security. It proposes that the shift to remote work may lead to an increased likelihood of cyber-attacks targeting telecommunication networks, systems, and sensitive data. This hypothesis implies that remote workers may weaken existing cyber security measures, exposing organizations in the telecommunications industry to a higher risk of cyber security incidents.

To test this hypothesis, data can be collected and analysed to assess the number and severity of cyber-attacks before and after the introduction of remote workers. The study also examined the specific vulnerabilities introduced by remote workers, such as increased reliance on home networks and personal devices, potential security gaps in remote access systems, and the impact of decreased physical security measures on protecting sensitive data. The research involved surveying telecommunication industry professionals, administering survey questionnaires, and analysing relevant statistical data to evaluate the extent to which remote workers affects cyber security in the industry.

The findings of this study will provide valuable insights into the relationship between remote worker and cyber security in the telecommunications industry. If the hypothesis is supported by evidence, it would underscore the importance of implementing robust

security measures and establishing effective policies to mitigate the increased cyber security risks associated with remote worker. On the other hand, if the hypothesis is not supported, it would indicate that remote workers do not significantly impact cyber security vulnerabilities and risks in the telecommunications industry, highlighting the effectiveness of existing security measures or the successful adaptation of security practices to remote worker environments.

1.7 Significance of the study

The study is significant as it contributes to the existing body of knowledge by focusing on a relatively understudied area, specifically the effects of Covid-19 on cybersecurity within the telecommunications industry in Zimbabwe. While there has been some research conducted on the impact of remote worker on cybersecurity globally, there are very few studies conducted in African countries, including Zimbabwe. By examining the Zimbabwean context, this study fills a critical gap in the literature and provides insights that are relevant to the local telecommunications industry.

The advent of the Covid-19 pandemic has forced organizations worldwide to rapidly adopt remote worker practices, including those in the telecommunications sector in Zimbabwe. This abrupt shift to remote workers has not only transformed work arrangements but has also brought about unique cybersecurity challenges. Understanding the specific effects of Covid-19 on cybersecurity within the telecommunications industry in Zimbabwe is essential for developing tailored strategies and interventions to address these challenges effectively.

By exploring the interplay between remote worker, Covid-19, and cybersecurity, this study will uncover the specific vulnerabilities, threats, and risks that have emerged in the telecommunications industry in Zimbabwe. It will examine the impact of Covid-19

on the effectiveness of existing cybersecurity measures and identify potential gaps or shortcomings that need to be addressed. Additionally, the study analysed the emerging cyber threats and attack vectors that have arisen because of the pandemic, considering the local context.

The findings of this study will have practical implications for organizations within the telecommunications industry in Zimbabwe. The insights gained will inform the development of targeted strategies, policies, and practices to enhance cybersecurity resilience in the face of the evolving remote work landscape. The study's contributions will extend beyond academia and provide valuable guidance to industry practitioners, policymakers, and regulators in Zimbabwe seeking to navigate the challenges posed by remote worker and bolster cybersecurity in a post-pandemic era.

Zimbabwe presents a unique context for studying the effects of Covid-19 on cybersecurity within the telecommunications industry. The country has its own distinct socio-economic, political, and technological landscape, which can influence the specific challenges and dynamics faced by organizations in this sector. By focusing on Zimbabwe, the study takes into consideration the local nuances and provides insights that are highly relevant to the country's telecommunications industry.

Limited Studies in African Countries: Despite the increasing importance of cybersecurity in remote worker environments, there is little research conducted in African countries, including Zimbabwe. By undertaking this study, it contributes to expanding the body of knowledge and expands the understanding of the specific cybersecurity challenges faced by the telecommunications industry in the African

context. The findings of the study will not only benefit Zimbabwe but also add to the broader knowledge base on cybersecurity in developing economies.

Practical Implications: The study's findings will have practical implications for organizations operating within the telecommunications industry in Zimbabwe. It will provide actionable insights and recommendations that can be used to strengthen cybersecurity measures, improve remote work policies, and enhance incident response capabilities. The study's outcomes will empower organizations to make informed decisions and investments to mitigate risks and protect sensitive data in the face of evolving cyber threats.

Pandemic Impact: The Covid-19 pandemic has brought significant disruptions to various sectors, including telecommunications. By examining the effects of Covid-19 on cybersecurity in the telecommunications industry in Zimbabwe, this study captures the immediate and long-term consequences of the pandemic. It investigates how the sudden shift to remote work has influenced the threat landscape, employee behaviours, and organizational cybersecurity practices. The study's findings will contribute to a better understanding of the lasting impact of the pandemic on cybersecurity in the telecommunications sector.

Policy and Regulatory Implications: The study's findings can inform policymakers and regulatory bodies in Zimbabwe about the specific cybersecurity challenges faced by the telecommunications industry in a remote work environment. It can guide the formulation of relevant policies, regulations, and guidelines to address these challenges effectively. By aligning policies with the study's recommendations, the government can promote a secure and resilient telecommunications sector, ensuring data protection, privacy, and continuity in the face of evolving cyber threats.

1.8 Delimitation of the study

This study is delimited in terms of its sample source and population. The research focuses on employees of a specific telecommunications company in Zimbabwe who worked remotely either full time or partially because of the COVID-19 pandemic. The sample population consists solely of individuals who were engaged in remote work within this telecommunications company during the pandemic period.

The decision to narrow the study's scope to employees of a single telecommunications company is driven by practical considerations, such as feasibility and access to data. By focusing on a specific organization, the study can delve deeper into the intricacies of remote work and cybersecurity within a well-defined context. However, it is important to acknowledge that the findings may not be fully representative of the entire telecommunications industry in Zimbabwe or other organizations within the sector.

The selection of employees who worked remotely as the sample population is based on the study's objective to investigate the effects of remote workers on cybersecurity within the telecommunications industry. By examining this specific group, the study can gather insights into the cybersecurity challenges, vulnerabilities, and risks associated with remote workers in the telecommunications context. It allows for a more targeted analysis of the impact of remote workers on cybersecurity within the chosen company.

It is essential to note that individuals who did not work remotely during the pandemic period are excluded from the study's population. This exclusion is made to maintain the study's focus on remote workers and its implications for cybersecurity. Therefore, the findings and conclusions of the study should be interpreted within the context of remote

workers and may not be directly applicable to non-remote workers within the telecommunications industry.

While this delimitation provides a focused and specific investigation into the effects of remote workers on cybersecurity within the telecommunications industry in Zimbabwe, it is important to recognize the limitations of generalizability to other organizations or sectors. Future research could expand the scope to include a broader range of organizations and industries to gain a more comprehensive understanding of the topic.

1.9 Limitation of the study

Response Rate: One limitation of this study is the potential difficulty in obtaining a high response rate from the target population. Since participation in the study was voluntary, there may have been a lack of motivation or incentive for respondents to take part. This could result in a lower response rate, which may affect the representativeness and generalizability of the findings. However, the researcher took measures to address this limitation by engaging in direct communication with the potential respondents. By explaining the value and purpose of the research and emphasizing the importance of their participation, the researcher aimed to encourage a higher response rate.

Interpretation of Questions: Another potential limitation is the possibility that respondents may have faced difficulties in interpreting and answering the research questions. The topic of cybersecurity can be complex, and respondents with varying levels of understanding or familiarity with the subject matter may have encountered challenges in providing accurate and meaningful responses. To mitigate this limitation, the researcher took steps to ensure clarity and simplicity in the language and structure of the questionnaire. By using clear and concise questions written in simple English,

the researcher aimed to facilitate respondents' comprehension and minimize interpretational difficulties.

Sensitivity of the Research Area: Given that the research area of cybersecurity can be sensitive, participants may have concerns about disclosing certain information or providing truthful responses. They may fear potential victimization or repercussions for their actions or practices related to cybersecurity. To address this limitation, the researcher took measures to establish trust and assure participants of the confidentiality and academic nature of the research. By emphasizing that the study is strictly academic and not intended as a job evaluation exercise, the researcher aimed to create a safe environment for participants to provide reliable and honest information.

Limited Generalizability: The findings of this study may be limited in terms of generalizability to other telecommunications companies or industries outside of the specific context of the chosen company in Zimbabwe. The unique characteristics, practices, and organizational culture of the selected company may not fully reflect the broader telecommunications industry or other organizations within the sector. Therefore, caution should be exercised when extrapolating the study's findings to wider populations or different contexts.

This study acknowledges several limitations, including potential challenges in obtaining a high response rate, difficulties in interpreting questions, concerns about disclosure, and limited generalizability. However, the researcher implemented strategies to mitigate these limitations, such as direct communication with participants, using simple language in the questionnaire, and establishing trust and confidentiality. Despite these limitations, the study provides valuable insights within its specific context

and contributes to the existing body of knowledge on the effects of remote workers on cybersecurity in the telecommunications industry in Zimbabwe.

CHAPTER 2 REVIEW OF RELATED LITERATURE

2.1 Introduction

This chapter is pivotal in understanding the significance of the research on the effects of remote workers on cybersecurity. It offers a comprehensive overview of existing knowledge, insights, and gaps in the field, providing essential context for the subsequent research chapters. This study employs Social Exchange Theory, Protection Motivation Theory (PMT), and the Technology Acceptance Model (TAM) to analyse cybersecurity in the context of remote work within the telecommunications industry. These theories help understand how employee perceptions of convenience, threat awareness, and technology usability influence their cybersecurity behaviours and practices, offering insights into developing more robust cybersecurity strategies.

Remote Workers

Remote workers are employees who work away from the office or from home according to N. E. M. Elshaiekh, Y. A. A. Hassan and A. A. A. Abdallah, (2018) there are different kinds of remote workers; According to the workers who use it, the place, type of work, the environment, and the purpose of use. According to the reviews there are positive and negative impacts on cyber security by using the remote workers.

During the COVID-19 pandemic there was a sudden shift in the way people work. (Tanpipat, 2021) For business continuity, many organizations have implemented a remote working policy for employees to work from home. Strategic facility management (FM) acted to support remote worker policies by developing organizational norms in an organization. Meanwhile, the human resource (HR) department chose to achieve business performance through remote workers by gaining job motivation among employees. However, there is limited understanding of how well

organizations adapted to remote workers , and what are the critical factors affecting their remote worker cyber security policy.

Several research papers showed that different assumptions are linked to remote worker because of the flexibility and autonomy granted to employees when working remotely or from home. This review consistently aims to describe remote work's role in employees' well-being and performance. Using the Preferred Reporting Items for Systematic reviews and Meta-analyses (PRISMA) guidelines, 20 peer-reviewed papers published from 2010 until 2021 were selected for this review. Findings showed various and mixed consequences on employees' performance and well-being. Specifically, remote working affects employees' perceptions about themselves and their workplaces and contributes to their physical and mental health, particularly regarding work-life balance.

A paper by A Georgiadou et al, examined the employee perceptions of remote working during the COVID 19 pandemic, focusing particularly but not exclusively on the rapid developments in cybersecurity for remote organisations and workers. Data was gathered from seven interviewees and forty-seven survey respondents who worked for the International Telecommunication Union under various contracts and in various positions at the time of the study. Studying the attitudes and experiences of remote workers uncovered that flexibility and time-saving efficiencies are the most valued benefits of remote working, while the lack of social interaction is seen as the worst feature of pandemic teleworking. An observed association between younger age and a reported decrease in motivation at work calls for further academic enquiry. While studied teleworkers did not experience cyberattacks in high volume, interview enquiry confirmed that cyberattacks adapted to the vulnerabilities of teleworking and intensified during the pandemic. Swift adaptations and increased employee cyber-protection likely

prevented further damage in the time of the Coronavirus cyber crisis but did not eliminate cyberattacks. The remaining cybersecurity vulnerabilities, especially in personal device usage, pose a permanent threat to organisational and personal safety, resilience and efficiency, (A Georgiadou, S Mouzakitidis, D Askounis - Security Journal,2022).

According to A Luna et al, Cyberslacking is conducted by employees who are using their company equipment and network for personal purposes instead of working during work hours. Cyberslacking has a significant adverse effect on overall employee productivity. Due to COVID 19 move to remote workers also pose a cybersecurity risk to organizations networks and infrastructure. In their research study, they developed, validated, and empirically tested a taxonomy to assess an organization, remote workers” risk level of cybersecurity threats. Their study included a three-phased developmental approach in developing the Remote Worker Cyberslacking Security Risk Taxonomy. In collaboration with cybersecurity Subject Matter Experts (SMEs) use the taxonomy to assess organization remote workers” risk level of cybersecurity threats by using actual system indicators of productivity measures to estimate their cyberslacking along with assessing via organizational information the computer security posture of the remote device being used to access corporate resources. results from 125 anonymous employees from one organization were assessed on the cybersecurity risk taxonomy where recommendation to the organizations cybersecurity leadership were provided, (A Luna, Y Levy, G Simco, W Li – 2022).

A paper by Sutherland explores the push in Africa for the widespread adoption of telecommunications and Internet which is aimed at boosting economic growth and access to digital government services. However, having significant effects on privacy by enabling surveillance of the networks, by allowing the collection of data about customers, their locations and transactions, which can be linked to other data and analysed for commercial or governmental purposes. Data can also be stolen or destroyed, by criminals, foreign powers, and terrorists. While countries have enthusiastically created telecommunications regulatory

authorities, they have only rarely created data protection authorities to oversee the collection, use and storage of data. They have also lagged on introducing strategies for cybersecurity and the centres needed to collect data on attacks and defences. Surveillance by secret police has grown in sophistication, with facilities for lawful interception, IMSI-catchers, and surveillance RATs, none of which is overseen by parliaments or the courts. Consequently, the rights to dignity and privacy are very poorly observed and more often breached. Sutherland, Ewan, Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance (June 22, 2018).

Shortly after the enthronement of COVID-19 on the global continent, cyberspace became a

dominant arena for social, economic, religious, educational, recreational and political activities across the world. A paper by Sogo Angel Olofinbiyi paper draws insights from the existing literature to illustrate how COVID-19 has provided situational opportunities for cyber criminals to strike and exploit people of their valuable resources through creating fraudulent websites as well as spreading of malware and ransomware

to vulnerable users. routine activity theory becomes very dominant and crucial in understanding the underlying basis for the increased cybercrimes that currently characterize the cyber space. Sogo Angel Olofinbiyi's study demonstrates that the twin phenomenon of coronavirus and cyber insecurity has not only instilled fears into the hearts of cyber users but has also negatively impacted the global economy in various ways that cannot be quantified by any study. Since all measures put in place to contain the threats of the horrible virus, have, hitherto, remained counterproductive, his paper recommended essential cyber hygiene practices (such as, antivirus protection, malware and phishing awareness, weak spots identification, intelligent techniques, risk management approach, zero trust design, home network security and general cybersecurity awareness) as a coping strategy to salvage both the public health and security sectors from the twin occurrence of Covid-19 pandemic and cyber insecurity, which has jeopardized significant portions of the global economy. Providing a continued cyber-safe remote-working environment for employees will be of ultimate measure. (Sogo Angel Olofinbiyi,2022).

The form of remote work organization was introduced in the 1980s and has so far been used to motivate and reward employees within the bonus system, reduce traffic congestion and the time it takes an employee to commute. Given the important role of information and communication technologies in the performance of their duties, this is also called telecommuting, but the definition also applies to jobs not related to ICT solutions. Due to the possibility of working from anywhere, remote workers are also called mobile workers, as it depends only on the availability of portable hardware such as wireless internet and a laptop (Ross, 2018).

According to Ross, (2018), remote workers can be classified as permanent or full-time, part-time (as needed, for example, by determining the frequency or amount of work to be performed remotely) and occasional or Hybrid (less than once a week).

Conceptually, remote work is different from “working from home” and from “forced working from home”. O’Connor et al, (2021) highlighted that not only do remote workers perform work tasks from their homes or official workplace, but also other places. The work from home concept foresees the individual choosing entirely how the work from home is organized; however, in contrast, forced working from home is described as transition to remote work in the impact of the COVID-19 pandemic. Therefore, it is necessary to separate voluntary remote work and COVID-19 forced remote work, where choice in favour of remote work is associated to epidemiological safety and restrictions introduced by governments. Furthermore, bearing in mind the swift shift towards more available remote work during the pandemic, there is a considerable influx of cyber incidents. Which have been observed in most of the enterprises in the Cisco (2020) study, where, depending on size of the company, most small and medium-sized companies (55%), and 60% of large companies perceived a growing trend of cyber incidents. The employee must adhere to cyber security protocols from the employer when working remotely.

This indicates the possibility of flexibility to adapt the work conditions for part-time or full-time remote work, but specific agreement must be arranged so the employees aware of the work conditions, subordination, specific training, policies, and control (International Labour Office, 2013). Personal devices are permitted for performing remote work, but contracts regarding use of private equipment (depreciation costs) must be in place. Common worldwide practice and local laws may state that specific costs can be stipulated in the relationship (for example: internet connection, use of a mobile

phone, electricity and other). Otherwise, there is a substantial capital investment by the worker – an interpretation of local labour laws in various countries may support the finding that the worker is an independent contractor, who may raise concerns about responsibility.

Similar labour laws regarding device use can be applied in countries worldwide with various

customization and need to adapt for critically important and specific examples, such as in the

European Union, where data processing, accountability, right of information and data security

must comply with General data protection regulation (Koch, 2020), availability of employee and working time control.

According to Ebula et al., (2014) There are four groups of operational cyber security risks in the Carnegie Mellon University classification that must be considered when introducing and providing remote work while creating policies, standards and ensuring that those are communicated with employees. These risks include System and technology risks, Non-compliance with internal procedures, Risks associated with human behaviour and human factors and Risks from external influences.

Businesses have been affected by cybercrime growth that includes social engineering. And attacks, which are even more possible because of telecommuting. events like pandemic can help cyber-criminals to exploit the situation for crafting cyber-crime campaigns. In the context of remote workers, companies and organizations must consider that employees may need to obtain and work with information classified

higher than the systems by which the remote work is performed. To adapt for work in higher cyber-risk circumstances (for example vulnerability of IT systems), it is necessary to incorporate the requirements of a cyber-security document as a policy in general (Ahmad, 2020).

During remote working companies need to find confidence in the compliance of the employee and physical workplace which can be achieved via specific requirements and guidelines that can be also called workspace standards (Hou et al., 2021). To foster cybersecurity during remote work companies should consider using wider multi-factor authentication methods, choosing not to use certain communication platforms, safe use of virtual private networks (VPN), and enhancing responsiveness to information technology security incidents (Škiljić, 2020). Moreover, mention should be made on the environment in which remote workers are conducting their respective tasks, as, during more strict epidemiological restrictions, workers are more susceptible to cyber incidents, which are less likely during informative and awareness-bringing campaigns (Buil-Gil et al., 2020). To be productive, effective, and cooperative as an individual it is crucial that companies implement successful change management by promoting teamwork. significant effect on perceived productivity and organizational commitment, while sustaining work demand. Moreover, employees' job motivation can sustain employees' commitment to the organization in a remote working context. These findings proposed the strategic FM guide, through which a remote working policy can further enhance FM practice. (Tanpipat, W., Lim, H. W., & Deng, X. 2021)

In 2016 Lilian M. De Menezes, Clare Kelliher carried a research on Flexible working Individual Performance, and Employee Attitudes whilst Comparing Formal and

Informal Arrangements. They examined the relationship between remote working and individual performance. They came up with several theories, they also examined potential indirect effects on employee performance through job satisfaction and organizational commitment and analysed whether these relationships differ depending on whether the arrangement was set up through a formal process or negotiated informally between the employee and the line manager. Survey data from 2,617 employees in four large organizations with well-established flexible working policies were collected and analysed. Their results showed average positive indirect effects from informal flexible working, but also negative direct effects from formal flexible working. They concluded that remote workers have a positive indirect effect via organizational commitment and job satisfaction on worker performance.

2.2 Theoretical framework

Social Exchange Theory: This theory proposes that social relationships are based on exchanges of resources and that individuals will engage in behaviours that maximize their rewards and minimize their costs. In the context of remote working and cyber security, this theory suggests that employees will weigh the benefits of working remotely, such as increased flexibility and reduced commuting time, against the risks of cyber threats and the costs of maintaining secure work practices. (Blau, 1964) For example, remote workers may be more willing to use personal devices for work-related tasks if it increases their convenience, even though this can increase the risk of a cybersecurity breach.

One study that supports the use of Social Exchange Theory in understanding the behaviour of remote workers is "Determinants of Teleworker Performance: A Theory

and Predictive Model," by Timothy Golden, Jennifer Veiga, and Steven Lautsch (2008). In this study, the authors found that teleworkers' performance was influenced by their perceptions of social support from colleagues and supervisors, as well as their perceptions of autonomy and control over their work. These factors are consistent with the principles of Social Exchange Theory, which emphasizes the importance of social relationships and perceived costs and benefits in determining behaviour.

Protection Motivation Theory (PMT) highlights that individuals will adopt protective behaviours if they sense a threat and believe that the behaviour will be effective in reducing the threat. In the context of remote workers and cyber security, this theory suggests that employees will be more likely to adopt secure work practices if they perceive cyber threats as a significant risk and believe that their actions can reduce the risk. (Rogers, 1975). This Theory seeks to explain how people respond to threats like those posed by cybersecurity risks. It suggests that people are motivated to adopt protective behaviours when they perceive a threat to their safety, health, or well-being, and when they believe that their actions can effectively reduce the threat. Employees will be more likely to adopt secure work practices if they perceive cyber threats as a significant risk and believe that their actions can reduce the risk. For example, employees may be more motivated to use strong passwords and update software if they understand the potential consequences of a cybersecurity breach and believe that these actions can reduce the risk of a breach.

Another study that supports the use of PMT in understanding employees' cybersecurity behaviour is "An empirical investigation of the antecedents of phishing awareness and

behaviour among university students: A protection motivation theory perspective," by Yanyan Deng, Yuanyuan Zhou, and Lan Wu (2020). In this study, the authors found that students' perceptions of the severity of phishing attacks, as well as their beliefs in their ability to avoid phishing attacks, were strong predictors of their awareness and behaviour related to phishing.

Technology Acceptance Model proposes that the adoption of new technology is influenced by perceived usefulness and perceived ease of use. In the context of remote workers and cyber security, this model suggests that employees will be more likely to adopt secure work practices if they perceive them as useful and easy to implement. (Davis, 1989)

The Technology Acceptance Model explain why individuals adopt or reject new technology. The model posits that an individual's intention to use technology is influenced by two primary factors: perceived usefulness and perceived ease of use.

Another study that supports the use of TAM in understanding employees' cybersecurity behaviour is "Examining Employees' Information Security Behaviours in the Context of Social Media: A Technology Acceptance Model Perspective," by Hui-Jen Yang, Chih-Ping Wei, and Chia-Chen Chen (2017). In this study, the authors found that employees' intentions to adopt secure behaviours related to social media use were strongly influenced by their perceptions of the usefulness and ease of use of the recommended security measures. These findings suggest that TAM can be used to understand cybersecurity behaviour in a variety of contexts, including remote work.

2.3 Relevance of the theoretical frame to the study

Bridging Theory and Research Objectives

The theoretical underpinnings of Social Exchange Theory, Protection Motivation Theory (PMT), and the Technology Acceptance Model (TAM) serve as a critical foundation for deriving the research objectives and questions central to this study. By applying these theories, we aim to dissect and understand the intricate behaviors and motivations of remote workers in the telecommunications industry regarding cybersecurity.

- **Social Exchange Theory** illuminates the personal calculus remote workers engage in when weighing the advantages of remote work against the potential cybersecurity risks. This perspective helps formulate research questions concerning the behavioral trade-offs employees are willing to make for the convenience of remote work and how these decisions impact cybersecurity risk.
- **Protection Motivation Theory (PMT)** focuses on the motivational drivers behind adopting cybersecurity measures, emphasizing threat perception and the belief in the efficacy of protective actions. From PMT, we derive questions regarding the extent to which threat awareness and confidence in cybersecurity practices influence employees' readiness to adopt these measures.
- **Technology Acceptance Model (TAM)** assesses the factors influencing the adoption of cybersecurity technologies and practices. It prompts us to question how perceptions of the usefulness and ease of implementing cybersecurity technologies affect their adoption among remote workers.

Crafting a Theoretical and Conceptual Framework

Building on these theories, the study constructs a theoretical and conceptual framework that guides the exploration of how remote work influences cybersecurity in the telecommunications industry. This framework not only informs the development of research objectives and questions but also provides a structured approach to analyzing the data collected. It encapsulates the relationship between employee behaviors, motivations, technology acceptance, and cybersecurity outcomes, offering a comprehensive lens through which to examine the study's key themes.

- The **theoretical framework** serves as a scaffold for understanding the dynamics of remote work and cybersecurity, integrating the theories to explore the nuanced behaviors and perceptions of employees.
- The **conceptual framework** translates these theoretical insights into a visual model, outlining the specific factors under investigation, such as the nature of remote work in the telecommunications industry, types of cyber threats, and the effectiveness of existing security measures. This model aids in pinpointing the interactions between these factors, facilitating a focused examination of their impact on cybersecurity.

By explicitly linking the chosen theories to the study's objectives and questions, this approach not only strengthens the research design but also ensures a solid foundation for defending the study's findings. It demonstrates a deliberate effort to apply theoretical insights to practical research challenges, laying the groundwork for a thorough investigation of the impact of remote work on cybersecurity within the telecommunications sector.

To complement these theories, a conceptual model could be developed that outlines the specific factors that influence the effects of remote workers on cyber security in the telecommunications industry. These factors could include:

Nature of the telecommunications industry: The telecommunications industry plays a pivotal role in modern society, serving as a critical infrastructure sector that enables essential communication services. Telecommunications companies facilitate the seamless transmission of phone calls, internet connectivity, data transfer, and video conferencing, connecting individuals, businesses, and organizations worldwide. Given the fundamental nature of their operations, these companies handle vast volumes of sensitive data, ranging from personal information to proprietary business data.

The security of telecommunications networks and data is of utmost importance in this industry. Safeguarding the integrity, confidentiality, and availability of telecommunications infrastructure and information is crucial to ensure the smooth functioning of communication services and maintain public trust. Cybersecurity breaches in the telecommunications industry can have severe consequences, with far-reaching implications.

One significant concern is the compromise of sensitive information. Telecommunications companies store and process a wealth of personal data, including customer records, billing information, and communication logs. In the wrong hands, such information can be exploited for identity theft, fraud, or other malicious activities. The unauthorized access, disclosure, or alteration of personal data can result in severe harm to individuals and erode public trust in the industry.

Moreover, the telecommunications industry's critical infrastructure status makes it an attractive target for cyberattacks. Disrupting the functioning of telecommunications

networks can have cascading effects on various sectors, including finance, healthcare, transportation, and emergency services. Such disruptions can impede economic activities, compromise public safety, and hinder emergency response efforts. Additionally, cyberattacks targeting telecommunications infrastructure can lead to significant financial losses for both companies and their customers.

Recognizing the criticality of cybersecurity in the telecommunications sector, industry standards and guidelines are in place to ensure the implementation of robust security measures. Organizations often adhere to frameworks provided by institutions such as the National Institute of Standards and Technology (NIST, 2021), which offer comprehensive guidance on cybersecurity best practices. These frameworks emphasize risk assessment, vulnerability management, incident response, and ongoing monitoring as essential components of a strong cybersecurity posture.

In conclusion, the telecommunications industry plays a vital role in facilitating communication and connectivity. Given the sensitive nature of the data handled by telecommunications companies and their critical infrastructure status, cybersecurity is of paramount importance. The industry faces significant risks from cyber threats, including the compromise of sensitive information, disruption of critical infrastructure, and financial losses. To mitigate these risks, robust cybersecurity measures, adherence to industry standards, and continuous vigilance are essential.

Types of cyber threats faced by remote workers: As remote work becomes increasingly prevalent, remote workers face a variety of cyber threats that can compromise the security of their devices, data, and networks. Understanding these threats is crucial for remote workers to take appropriate measures to protect themselves

and their organizations. Here are further expansions on the types of cyber threats faced by remote workers:

- **Phishing Attacks:** Phishing attacks are a common and pervasive threat for remote workers. Cybercriminals use deceptive emails, instant messages, or text messages disguised as legitimate communications to trick individuals into divulging sensitive information such as usernames, passwords, or financial details. Phishing attacks often employ social engineering techniques, exploiting human emotions and creating a sense of urgency to manipulate users into taking actions that benefit the attackers. These attacks can lead to identity theft, unauthorized access to accounts, or the installation of malware.
- **Malware:** Malware is malicious software designed to infiltrate and compromise remote workers' devices. It includes various types such as viruses, spyware, and ransomware. Viruses can replicate and spread, damaging files and disrupting system operations. Spyware is designed to collect information without the user's knowledge, including keystrokes, login credentials, and browsing habits, which can be used for identity theft or other malicious purposes. Ransomware encrypts files on a victim's device, rendering them inaccessible until a ransom is paid. Malware can be accidentally downloaded through malicious email attachments, infected websites, or compromised software, posing a significant risk to remote workers' data and privacy.
- **Unauthorized Access:** Remote workers may face the risk of unauthorized access to their devices, networks, or sensitive information. This can occur when remote workers connect to unsecured public Wi-Fi networks that are

vulnerable to eavesdropping or man-in-the-middle attacks. Cybercriminals can intercept communications, capture login credentials, or gain unauthorized access to confidential data. Additionally, weak or reused passwords can be exploited through brute-force attacks or credential stuffing, allowing unauthorized individuals to enter systems or accounts.

- **Virtual Private Network (VPN) Vulnerabilities:** Remote workers often rely on VPNs to establish secure connections to their organization's network. However, VPNs can also introduce vulnerabilities if they are not properly configured or if remote workers connect to untrusted VPN services. Inadequate encryption, misconfigurations, or outdated VPN software can be exploited by attackers to intercept or manipulate network traffic, granting unauthorized access to sensitive data.
- **Social Engineering Attacks:** Social engineering attacks target remote workers by exploiting their trust, curiosity, or willingness to help. Attackers may impersonate colleagues, IT support personnel, or trusted individuals to deceive remote workers into revealing sensitive information or performing actions that compromise security. Social engineering techniques include pretexting, baiting, or phishing via phone calls, emails, or fake websites.

To mitigate these cyber threats, remote workers should adopt proactive security measures such as:

- Being vigilant and cautious when receiving unsolicited emails, messages, or requests for sensitive information.
- Verifying the authenticity of communications and avoiding clicking on suspicious links or downloading attachments from unknown sources.

- Keeping devices and software up to date with the latest security patches and antivirus software.
- Using strong and unique passwords or password managers and enabling multi-factor authentication.
- Connecting to secure and trusted Wi-Fi networks or using a VPN with robust encryption when working remotely.
- Regularly backing up important data and files to protect against data loss in the event of a cyber incident.
- Staying informed about the latest cybersecurity threats and best practices through awareness training programs.

By understanding the types of cyber threats faced by remote workers and implementing appropriate security measures, individuals can reduce the risk of falling victim to cyberattacks and help protect their own and their organization's sensitive information, (NIST, 2021).

The effectiveness of existing security measures such as firewalls, antivirus software, and access controls, can be compromised when it comes to remote working. While these measures are designed to protect devices, networks, and data, the unique challenges posed by remote work can introduce vulnerabilities and undermine their efficacy. Here are further expansions on the factors that can compromise the effectiveness of these security measures:

1. **Configuration Challenges:** Firewalls and access controls, which act as barriers between internal networks and external threats, may not be properly configured to protect remote workers' devices. In a traditional office environment, these

security measures are typically implemented at the network perimeter. However, with remote work, the network perimeter extends to employees' homes, coffee shops, or other locations outside the direct control of the organization. Ensuring that firewalls and access controls are correctly set up to secure remote connections can be challenging, especially if organizations lack the necessary resources or expertise.

2. **Outdated or Inadequate Antivirus Software:** Antivirus software is a critical defence mechanism against malware and other malicious software. However, remote workers may not have the same level of protection as they would in an office environment. Antivirus software may not be regularly updated on remote devices, leaving them vulnerable to new and emerging threats. Furthermore, remote workers may use personal devices that lack robust antivirus software altogether, increasing the risk of infection and compromising the security of both personal and corporate data.
3. **Lack of Awareness and Adherence to Security Protocols:** Remote workers may not be fully aware of the organization's security protocols or may fail to follow them consistently. This can range from neglecting to use secure passwords and multi-factor authentication to disregarding guidelines for handling sensitive data or accessing corporate resources. The absence of physical oversight and the potential blurring of personal and professional boundaries in remote work environments can contribute to lax security practices. Even with robust security measures in place, if remote workers do not adhere to protocols, the effectiveness of those measures is diminished.

4. **Increased Attack Surface:** Remote workers expands the attack surface for cybercriminals. With employees accessing corporate resources from various locations and devices, the potential entry points for attacks multiply. Cybercriminals may specifically target remote workers who may have weaker security measures in place compared to office networks. This increased attack surface puts a strain on existing security measures, as they need to cover a broader range of devices, networks, and potential vulnerabilities.

Addressing the compromised effectiveness of security measures in remote work requires organizations to adapt and enhance their security strategies. Some key considerations include:

- Ensuring remote workers have access to updated and properly configured security tools, such as firewalls, VPNs, and antivirus software, on their devices.
- Providing clear and comprehensive security guidelines and awareness training to remote workers, emphasizing the importance of adhering to security protocols.
- Implementing remote access controls and authentication mechanisms that are specifically designed for remote work scenarios, such as multi-factor authentication and secure remote desktop solutions.
- Regularly assessing and updating security measures to address the evolving threat landscape and the changing needs of remote work environments.
- Encouraging remote workers to report any security incidents or concerns promptly, fostering a culture of vigilance and accountability.

By addressing the unique challenges of remote work and implementing tailored security measures, organizations can mitigate the risks associated with compromised security effectiveness and enhance the overall security posture for remote workers. (Tipton & Nozaki, 2019)

The theoretical framework of this study highlights the paramount importance of human behaviour, perceptions, and attitudes in the realm of cybersecurity, particularly in the context of remote working. It emphasizes that while technological measures are essential, the actions and mindset of employees play a significant role in determining the effectiveness of cybersecurity measures.

The framework recognizes that cybersecurity risks ultimately lie in the hands of employees. Their work behaviour and the prevailing organizational culture significantly influence their level of vigilance and commitment to mitigating cyber risks. Employees who are aware of the potential consequences of cyber threats and perceive them as significant are more likely to adopt security best practices, adhere to policies, and remain vigilant in detecting and reporting potential incidents.

Perceptions and attitudes towards cybersecurity are crucial factors that shape employee behaviour. Individuals' understanding, beliefs, and awareness of cybersecurity threats directly impact their actions and decision-making. Moreover, employees' overall stance and inclination towards cybersecurity practices, reflected in their attitudes, play a vital role in their motivation, willingness, and commitment to following security protocols.

The study recognizes that fostering a strong cybersecurity culture within organizations is essential. A culture that prioritizes cybersecurity, provides regular training and awareness programs, and encourages a shared responsibility for security can significantly influence employees' behaviours and attitudes. By cultivating such a

culture, organizations can promote security awareness, proactive engagement with cybersecurity practices, and a sense of responsibility among their employees.

The implications of this theoretical framework are particularly relevant in the context of remote workers. As remote work introduces new challenges and vulnerabilities, employees' behaviours and attitudes become even more critical. Factors such as adhering to secure remote access protocols, being aware of phishing attacks, protecting sensitive data, and ensuring secure handling of devices and networks heavily rely on employees' actions and understanding.

2.4 Summary

Chapter 2 delves into the critical frameworks guiding the study which mainly emphasise on the role of human behaviours, perceptions, and attitudes in the realm of cybersecurity risk management, particularly in the context of remote workers. It underscores the necessity for employees to be not only vigilant but also proactive in identifying and mitigating potential cyber threats. This proactive stance is essential in the contemporary landscape where remote work has become increasingly prevalent, bringing with it unique cybersecurity challenges.

The chapter highlights the importance of developing a robust cybersecurity culture within organizations. Such a culture is fundamental in fostering secure practices and enhancing overall awareness among employees. This cultural shift is not merely about implementing policies or procedures; it's more about ingraining cybersecurity as a fundamental aspect of the organizational ethos and daily work practices.

In emphasizing human-related factors, the chapter points out that while technical defences are crucial, the human element cannot be overlooked. Employees are often the first line of defence against cyber threats, and their actions can significantly impact an organization's cybersecurity posture. Therefore, training and awareness programs are essential to equip them with the necessary skills and knowledge to recognize and respond to cyber threats effectively.

Furthermore, the chapter discusses how organizations can adapt to the evolving nature of cyber risks in remote work settings. It suggests that a combination of employee education, strong policy frameworks, and a culture of security is vital for effectively managing these risks.

In summary, Chapter 2 of the study articulates that addressing human elements — behaviour, perception, and attitudes — is crucial for enhancing cybersecurity in the modern context of remote work. It argues that by focusing on these aspects, organizations can significantly bolster their defences against cyber threats, thereby maintaining a strong and resilient cybersecurity posture.

CHAPTER 3 METHODOLOGY

3.1 Introduction

In this chapter, we detail the quantitative methodology that frames our investigation into the cybersecurity implications of remote work within the telecommunications sector in Zimbabwe. A structured approach, utilizing survey questionnaires, was adopted to collect quantifiable data, enabling statistical analysis for precise and generalizable findings. This method aligned with our goals to examine patterns, relationships, and trends across a broad sample, providing a systematic and objective basis for our analysis.

The quantitative approach methodology used hinges on the deployment of survey questionnaires to gather standardized data across diverse demographic and professional segments within the industry. This approach ensures a wide-ranging representation, critical for the reliability and validity of the research findings. The decision to conduct surveys online expanded my reach beyond Harare, facilitating a comprehensive national perspective.

3.1.1 Quantitative Research

This study made use of survey questionnaires. According to Wilfred Uronu Lameck, (2013), surveys questionnaires were reliable and valid for proper sampling techniques were employed. The sample population was a true representative of the population. In my sampling for the survey questionnaires, I ensured that all age groups are represented, all departments and sections are represented and that all levels of employees are represented to ensure that I cover all sections within the organisation. The surveys and

questionnaire were administered online, and this enabled me to reach out all over Zimbabwe and not just Harare I composed the relevant questions and send a link to the sample population so that they can open the link and respond to the survey questions. According to M. Siva Durga Prasad Nayak¹, K.A. Narayan, (2019) using online questionnaires is cheaper and quick to analyse for the researcher and for the participants it was easy to use, and more honest and accurate answers were provided because it was an anonymous response.

This research leans heavily on quantitative methods, characterized by their systematic, objective approach, allowing for high precision in examining relationships and patterns. The study utilizes advanced statistical techniques to infer about the larger population from the sample data, contributing significantly to the understanding of variable quantification, trend identification, and drawing generalizable conclusions. In this study, a robust quantitative research methodology was employed, primarily utilizing survey questionnaires as the key tool for data collection. The quantitative approach, selected for its suitability in systematically gathering numerical data, enables detailed statistical analysis and the generation of precise results. This approach is particularly effective for analysing relationships, patterns, and trends across a substantial sample size, aligning with the study's objectives to explore the broad effects of remote workers on cybersecurity.

The survey questionnaires are meticulously designed to elicit structured, standardized data suitable for quantitative analysis. This systematic collection is crucial for the investigation of remote work's cybersecurity implications within the telecommunications sector.

3.2 The research design

The research design employed in this study is a cross-sectional descriptive design, which was particularly suited for exploring and documenting the current state of cybersecurity practices within the telecommunications industry amid the shift to remote working. This design allowed for the collection of data at a single point in time, offering a snapshot of practices, challenges, and attitudes towards cybersecurity among remote workers within the sector.

Justification for the Cross-Sectional Descriptive Design

1. **Appropriateness for the Research Objective:** The primary aim of the study is to assess the effects of remote workers on cybersecurity within the telecommunications industry. A cross-sectional descriptive design was appropriate as it enabled the researcher to measure and describe the variables of interest as they exist in a specific moment, which is crucial for understanding the current cybersecurity landscape (Babbie, 2016).
2. **Efficiency in Data Collection:** Given the broad scope of the telecommunications industry and the diverse population of remote workers, this design facilitated efficient data collection across different segments of the industry. It allowed for the gathering of data from many respondents in a relatively short period, making it a cost-effective approach for the study (Creswell & Creswell, 2017).
3. **Facilitates Comparative Analysis:** This design supported the comparison of cybersecurity practices, perceptions, and challenges across different demographics, job roles, and company sizes within the telecommunications sector. Such comparisons revealed important insights into how cybersecurity

is impacted by remote workers across the industry (Cooper & Schindler, 2014).

4. **Foundation for Future Longitudinal Studies:** Although cross-sectional in nature, the design lays the groundwork for future longitudinal studies by establishing baseline data. Researchers can use the findings from this study to track changes and trends over time, contributing to a deeper understanding of how remote workers continues to affect cybersecurity in the telecommunications industry (Fowler Jr, 2013).
5. **Versatility in Analyzing Varied Data Types:** The descriptive nature of this design allows for the analysis of both quantitative and qualitative data, providing a comprehensive view of the cybersecurity landscape. This is particularly useful in understanding complex phenomena like cybersecurity, where both statistical trends and personal perceptions are important (Maxwell, 2012).

Sampling

Survey Sampling: Stratified random sampling technique was utilized to ensure a comprehensive representation of various segments within the telecommunications industry. This sampling approach ensured diversity and relevance in the participant selection, enhancing the study's generalizability and accuracy. Stratified random sampling technique was employed to select participants who have experience working in the telecommunications industry in Zimbabwe and have been engaged in remote working during the research period. The sample size was determined based on statistical power analysis and the availability of participants.

3.3 Population and Sampling

Study Population

The population of interest for this study includes employees and organizations within the telecommunications industry who have transitioned to remote work arrangements. It encompasses various job roles such as network administrators, IT professionals, cybersecurity experts, and employees handling sensitive information within EcoCash.

Sampling Techniques:

Stratified Random Sampling: To ensure representation from different segments of the population, stratified random sampling was utilised. The telecommunications industry was divided into strata based on factors such as company size, geographical location, and job roles. A proportionate number of participants was then randomly selected from each stratum.

Sample Size

Cooper and Schindler (2014) define a sample size as a group of respondents who are part of an overall target population that was selected carefully to represent a population. A sample size allows a researcher to draw valid conclusions on the research objectives that were formulated at the start of the study. To calculate the sample size for a survey in Ecocash Holdings with 750 employees, we can use a formula known as the sample size calculation for a finite population. Here's the breakdown:

- Identify the population size (N): In this case, the population size is 750 employees.
- Determine the desired level of confidence (C): The desired level of confidence refers to the level of certainty we want to have in the survey results. Common

confidence levels are 95% or 99%. Let's assume a confidence level of 95% (which corresponds to a confidence coefficient, Z, of 1.96).

- Specify the margin of error (E): The margin of error is the maximum acceptable difference between the survey estimate and the actual population value. Choose an appropriate margin of error based on the desired precision. Let's assume a margin of error of 5% (0.05).

Calculate the sample size (n): Using the following formula:

$$n = (Z^2 * p * q) / (E^2 / (N - 1) + Z^2 * p * q)$$

where: Z = Z-score corresponding to the desired confidence level (1.96 for 95% confidence) p = Estimated proportion of the population with a certain characteristic (use 0.5 for maximum variability if no estimate is available) q = 1 - p (complement of p) E = Margin of error N = Population size

Applying these values to the formula, we get:

$$n = (1.96^2 * 0.5 * 0.5) / ((0.05^2 / (750 - 1)) + (1.96^2 * 0.5 * 0.5))$$

Simplifying the equation:

n ≈ 278 is the sample size

3.4 Data collection instruments

Survey Questionnaires :

A survey questionnaire was used and allows researchers to collect a large amount of data efficiently and systematically. It enables gathering information from a diverse range of respondents within the telecommunications industry, including employees, IT

professionals, and managers. The questionnaire was distributed electronically, making it accessible to a geographically dispersed workforce. Survey questionnaires were selected for their efficiency in collecting large-scale data. They were designed to encompass a wide array of cybersecurity aspects relevant to remote working. The use of electronic distribution methods enhances reach and participation, allowing for a more diverse and comprehensive data set.

Surveys provided quantitative data, allowing for statistical analysis and quantitative comparisons. By using structured questions with predefined response options, the researchers could measure and quantify the effects of remote workers on cybersecurity within the telecommunications industry. This facilitates identifying trends, patterns, and relationships between variables, offering valuable insights for decision-making.

A well-designed survey questionnaire covered a broad range of cybersecurity aspects related to remote working in the telecommunications industry. It explored various dimensions, such as the effectiveness of security measures, awareness of security protocols, challenges faced by remote workers, and the prevalence of cyber threats. This comprehensive understanding helps in identifying specific areas that require attention or improvement.

The surveys provided consistency in data collection. By using the same set of questions for all respondents, the researcher ensured standardized data, which enhances comparability and reduces bias. This enabled a more accurate analysis of the overall effects of remote workers on cybersecurity within the telecommunications industry.

Surveys offered a level of anonymity to participants, encouraging honest and objective responses. Remote workers may feel more comfortable sharing their experiences, challenges, and perceptions related to cybersecurity without fear of retribution.

Anonymity promotes data integrity and allows for a more accurate representation of the workforce's views and experiences.

Conducting a survey questionnaire was a cost-effective and time-efficient research method. It eliminated the need for face-to-face interviews or focus groups, which can be logistically challenging and time-consuming, especially when dealing with a geographically dispersed workforce. Surveys were administered electronically, saving time and resources while reaching many respondents simultaneously.

Basis for Future Research: The data collected through a survey questionnaire can serve as a foundation for future research and analysis. Researchers can use the findings to generate hypotheses, explore relationships between variables, and identify areas that require further investigation. The data can also inform the development of targeted interventions and strategies to enhance cybersecurity practices within the telecommunications industry.

Overall, a survey questionnaire was a valuable research tool for investigating the effects of remote workers on cybersecurity within the telecommunications industry. It enabled the researcher to gather quantitative data, gain comprehensive insights, and identify areas for improvement. The findings can inform decision-making, policy development, and the implementation of effective cybersecurity measures in the context of remote work.

Online surveys were distributed to the selected participants using email or online survey platforms. The questionnaires included both closed-ended and open-ended questions to gather quantitative and qualitative data on the effects of remote workers on cybersecurity.

3.5 Analysis and organization of data

Quantitative Data Analysis: In the research study, the quantitative data collected through survey questionnaires was subjected to data analysis using statistical software, such as the Statistical Package for the Social Sciences (SPSS). The purpose of quantitative data analysis is to derive meaningful insights, patterns, and relationships from the numerical data collected in the study.

Descriptive Statistics: were used to summarize and describe the characteristics of the collected data. Common descriptive statistics include frequencies, percentages, means, and standard deviations. Frequencies provided a count of how often each response option was chosen for a specific question, while percentages represent the proportion of participants selecting each response option. Means and standard deviations provided measures of central tendency and variability, respectively, for continuous variables.

For example, the survey questionnaire included a question about participants' age, descriptive statistics would be computed to summarize the age distribution of the sample. This could involve calculating the frequencies and percentages of participants within different age ranges, as well as the mean and standard deviation of the overall age.

Inferential statistics: were used to draw conclusions and make inferences about the larger population based on the collected sample data. These statistical techniques examined relationships and associations between variables, helping to determine if the observed patterns in the sample are likely to be representative of the broader population. Common inferential statistical techniques include correlation analysis, t-tests, and chi-square tests. Correlation analysis examined the strength and direction of the relationship

between two continuous variables. It quantified the degree to which changes in one variable were associated with changes in another.

T-tests were used to compare means between two groups or conditions. They determined if the observed differences between the groups were statistically significant or if they could have occurred by chance.

Chi-square tests, on the other hand, examined the association between categorical variables. They assess whether the observed frequencies of different response options are significantly different from what would be expected by chance.

For instance, if the research study aimed to investigate the relationship between remote work experience and job satisfaction, inferential statistical techniques, such as correlation analysis or t-tests, may be employed to examine the strength and significance of the relationship between these variables.

Overall, quantitative data analysis involved applying appropriate statistical techniques to the collected numerical data. Descriptive statistics summarized the characteristics of the data, while inferential statistics help draw meaningful conclusions and make inferences about the larger population based on the sample data. These analyses contributed to uncovering patterns, relationships, and associations that support the research objectives and address the research questions.

3.6 Ethical Consideration

Special or vulnerable populations:

In the research study, random sampling was utilized to select research participants, ensuring that everyone had an equal chance of participating in the research. This approach was employed to minimize bias and discrimination in participant selection. The sample might have included disabled people. To address the ethical concerns associated with special or vulnerable populations, specific measures were taken during participant selection, data collection, and data handling. These measures aimed to ensure the inclusion, protection, and fair treatment of all participants, regardless of their characteristics or vulnerabilities.

Payment (if any) to be paid to each participant:

In the research study, no payments were made to the participants for their involvement. Instead, the participants volunteered to participate in the research on a voluntary basis. This information was disclosed to them at the beginning of the study, ensuring transparency about the absence of monetary compensation. It was important to ensure that participants are fully aware of the voluntary nature of their involvement. This included providing clear information about the absence of payment and any potential benefits or impacts of their participation. Overall, in the described research study, participants volunteered their time and involvement without receiving any payment. This decision was communicated clearly to the participants, and appropriate measures were taken to ensure their informed consent and understanding of the voluntary nature of their participation.

Informed Consent:

In the research study, obtaining informed consent from all participants was a crucial step before their participation. The process of informed consent involved briefing

participants on the research topic, purpose, procedures, and any potential risks or benefits associated with their involvement.

Specifically, participants were informed that the research study was conducted for academic purposes only, meaning that the data collected would be used for research and educational purposes rather than for commercial or monetary gain. They were explicitly notified that no payments or financial compensation would be made to participants in exchange for their participation.

Furthermore, participants were made fully aware of their right to withdraw from the study at any given point if they felt discomfort, dissatisfaction, or any other reason that made them no longer wish to continue their participation. This emphasized the voluntary nature of their involvement and ensured that participants felt empowered to exercise their right to discontinue their participation without any negative consequences or penalties.

The informed consent process is crucial for upholding ethical standards in research and protecting the rights and autonomy of participants. It ensures that participants have a clear understanding of what their involvement entails, what is expected of them, and what they can expect from the research study. This process promotes transparency, trust, and respect between researchers and participants, ultimately contributing to the ethical conduct of the study.

Potential Risks:

There are no risks or harm that may be posed by the research study to the participants.

Confidentiality/privacy:

Specific ethical standards are used in the research to guarantee that none of the volunteers were ever exposed to any harm that could have harmed or destroyed their reputations or professions. All research participants' identities had to be kept secret during the study. Although the respondents gave personal information, there was no part in which they had to fill out their names or any other details that could be used to individually identify them. Second, the surveys and email data were solely accessible to the researcher. This information was not accessible to any outside parties. These extreme measures made sure that the research participants' identities were kept a secret both during and after the study.

I was careful to avoid creating or misrepresenting the data that was used for the analysis of the study. Copyright policies were followed and all writers whose work was referenced in this study will be given proper acknowledgment on the reference page and in-text citations.

During the data collection procedure, it was crucial for the study to uphold moral conduct and foster confidence between the researcher and the subjects. I was open about the topic and goal of the study.

3.7 Summary

This chapter outlined the methodology used to study the effects of remote worker on cybersecurity within Zimbabwe's telecommunications industry. Employing a quantitative approach, we analysed responses from 230 employees, chosen from a sample population of 278 people through stratified random sampling from a total population of 750. Data collection was facilitated via structured questionnaires, blending both closed and open-ended queries to gather diverse insights. The analysis utilized SPSS for both descriptive and inferential statistics, ensuring a thorough

examination of the data. To guarantee reliability and validity, the questionnaire underwent pilot testing, and ethical considerations such as informed consent, voluntary participation, and privacy were rigorously maintained throughout the study.

CHAPTER 4: DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

4.1 Introduction

This chapter presents an in-depth analysis and interpretation of the data collected during the research, which specifically focuses on the effects of remote worker on cybersecurity within the telecommunications industry. The research aimed to provide a comprehensive understanding of the potential risks and challenges associated with remote work in relation to cybersecurity, as well as identify effective strategies for mitigating these risks.

4.2 Data presentation and analysis

Given the 230 responses, we observe the following:

- $230 \times 0.30 = 69$ respondents to report cybersecurity incidents (Expected "Yes")
- $230 \times 0.70 = 161$ respondents to report no incidents (Expected "No")

Using these numbers, we can perform a chi-squared test with the observed frequencies from the data:

- Observed "Yes" (reported incidents): 116
- Observed "No" (no incidents reported): 114

Let's calculate the chi-squared statistic and interpret the results to evaluate the hypothesis. We'll use a significance level of 0.05 for the test. If the p-value is less than 0.05, we'll reject the null hypothesis (H_0) in favor of the alternative hypothesis (H_1).

Based on the hypothetical expected frequencies and the observed frequencies from the data, we have calculated the chi-squared statistic and the corresponding p-value. Here are the results of the chi-squared test:

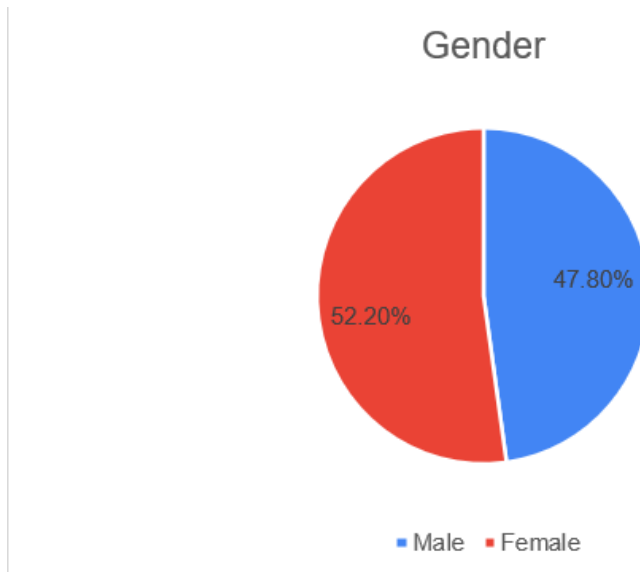
- Chi-squared statistic: 19.97
- Degrees of freedom: 1
- p-value: 7.85×10^{-6}

The chi-squared statistic indicates how much the observed frequencies deviate from the expected frequencies. The p-value tells us the probability of observing this deviation (or a more extreme one) by chance if the null hypothesis were true. With a p-value much lower than the significance level of 0.05, we reject the null hypothesis (H0).

In the context of this analysis, this means that the data provides strong evidence to support the alternative hypothesis (H1): The introduction of remote workers in the telecommunications industry has a significant impact on cyber security vulnerabilities and risks, resulting in an increase in the number and severity of cyber-attacks.

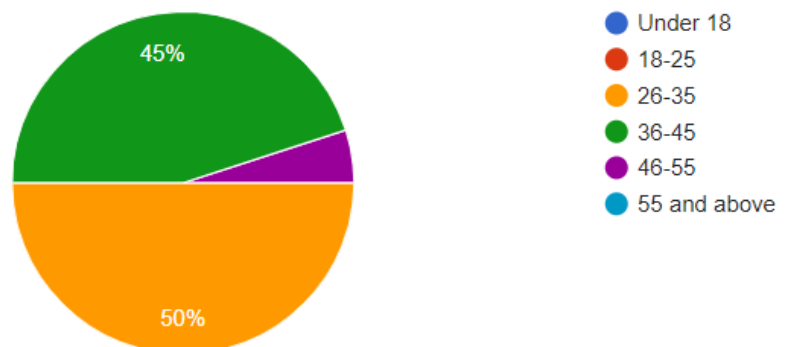
4.2.1 Response Rate Analysis

From a sample target of 278 participants, we received responses from 230 individuals, resulting in a response rate of 82.7%. This response rate exceeded the recommended threshold of 67% set by Saunders et al. (2009), indicating the reliability of our data. The high response rate strengthens the validity of our research findings.



Out of the total respondents, 47.80% are Male. This indicates that slightly less than half of the participants are male. The remaining 52.20% of respondents are Female, suggesting that just over half of the participants are female. This distribution shows a slightly higher representation of females in the research.

Age:



Descriptive Analysis:

The largest age group among the respondents is the "26-35" category, making up 50% of the sample. This indicates that half of the respondents fall within this age range, suggesting a relatively young respondent pool. The second-largest group is

"36-45", constituting 45% of the respondents. This shows that a significant portion of the respondents are in the mid-career stage. All other age groups, such as "Under 18", "18-25", "46-55", and "55 and above", make up a very small portion of the sample (the remaining 5%), with each of these categories being less than 5% since they are not individually labeled in the chart. This suggests that these age groups are minimally represented or not represented at all in the research sample.

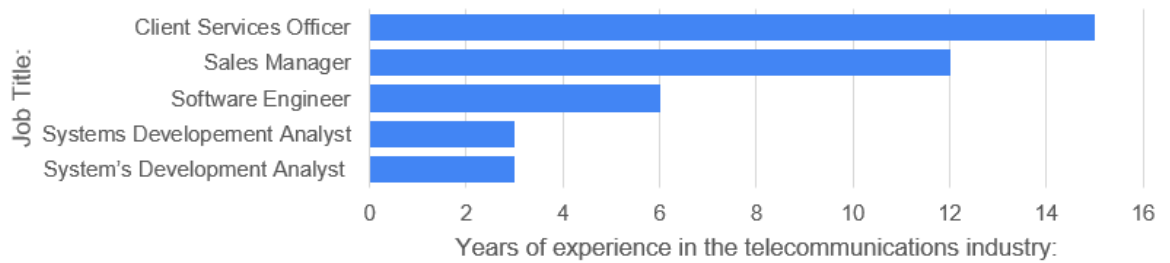
Statistical Analysis:

Given the predominance of the "26-35" and "36-45" age groups, the sample may not be representative of populations where a more even age distribution is expected. The total number of respondents is 230, we can estimate the number of people in each age group. For instance, 50% of 230 is 115 people in the "26-35" age group, and 45% is 103.5, which we would round to either 103 or 104 for the "36-45" age group. The age distribution of the respondents is heavily skewed towards the "26-35" and "36-45" age groups. If these demographics align with the research objectives, the findings will be particularly relevant for these age groups. However, the underrepresentation of other age groups should be acknowledged as a limitation in terms of the breadth of applicability of the research outcomes. The insights gained from this research will be most applicable to young to middle-aged adults.

4.2.2 Findings on Remote Work and Cybersecurity

The data gathered from employees in the telecommunications industry reveals that remote work has had a significant impact on cybersecurity awareness. A substantial proportion of respondents reported an increased understanding of cybersecurity risks

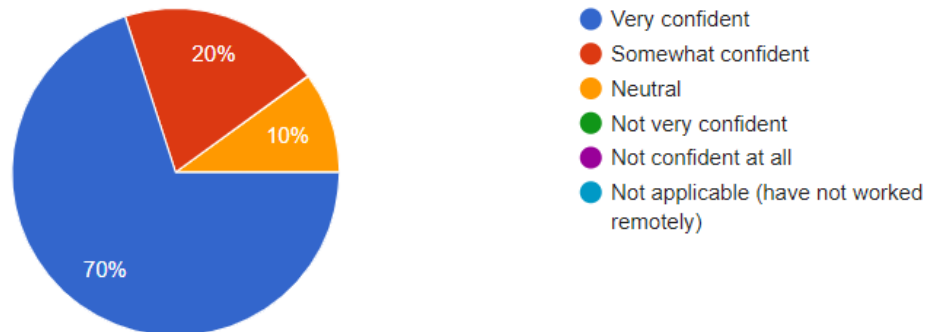
associated with remote work. This finding underscores the importance of remote work in shaping employees' perceptions of cybersecurity threats.



Summary of the raw data:

- Those who prefer to work only from the office have an average of 15 years of experience.
- Those who prefer a mix of remote and office-based work have an average of approximately 8.87 years of experience.
- Those who prefer to work exclusively remotely have an average of approximately 7.38 years of experience.
- The grand total average years of experience across all groups is approximately 8.53 years.

How confident are you in your ability to identify and respond to cyber security threats while working remotely?



Descriptive Analysis:

- **Very Confident:** Most respondents, 70%, feel very confident in their ability to identify and respond to cybersecurity threats while working remotely. This indicates a high level of self-assessed cybersecurity awareness or competence among the majority.
- **Somewhat Confident:** 20% of respondents are somewhat confident, suggesting that while they may have some awareness or skills, they acknowledge there is room for improvement or uncertainty in certain situations.
- **Neutral:** A smaller group, 10%, is neutral, neither confident nor unconfident. This could indicate a lack of experience or knowledge about cybersecurity, or uncertainty about their abilities.
- **Not Very Confident / Not Confident at All / Not Applicable:** These categories are not explicitly shown in the provided chart, which could imply that their percentages are very small or zero. If we're only considering the percentages

shown, none of the respondents fell into these categories, or they were too small a number to be quantified separately in the pie chart.

Statistical Analysis:

With the provided percentages, if we again consider a total of 230 respondents, we can estimate the number of respondents in each confidence category.

"Very Confident": 70% of 230 is 161 respondents.

"Somewhat Confident": 20% of 230 is 46 respondents.

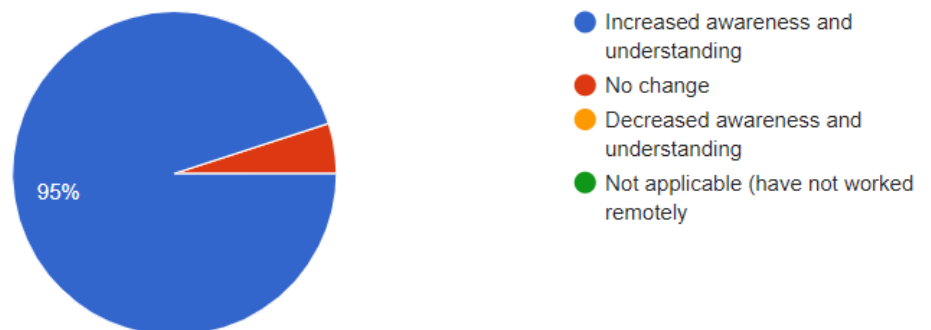
"Neutral": 10% of 230 is 23 respondents.

The confidence levels are ordinal data, so we could calculate measures like the median or mode but not the mean. The mode here is "Very Confident," and the median would likely fall into the "Very Confident" category as well, given the distribution.

4.2.3 Findings on Cybersecurity Measures

Most respondents noted an improvement in their organization's cybersecurity posture. This improvement is attributed to various factors, including comprehensive training and the implementation of secure network connections. These findings suggest that telecommunications companies have been proactive in addressing cybersecurity concerns in the context of remote work.

How has remote working affected your awareness and understanding of cyber security risks?



Descriptive Analysis:

A vast majority of respondents, 95%, report that remote working has increased their awareness and understanding of cybersecurity risks. This indicates a significant positive impact on cybersecurity consciousness among these individuals. A very small portion of the pie chart, which is not explicitly labeled with a percentage, indicates that there are respondents who have experienced no change in their awareness and understanding of cybersecurity risks due to remote working. Given the dominance of the 'Increased awareness' category, this group is likely very small. The categories for 'Decreased awareness and understanding' and 'Not applicable (have not worked remotely)' are not visible in the chart, suggesting either no respondents fell into these categories, or the number was too small to be represented.

Statistical Analysis:

The total number of respondents is 230, we can infer that approximately 218.5 respondents (which we would round to either 218 or 219) feel that their awareness and understanding of cybersecurity risks have increased due to remote working.

The remaining respondents (either 11 or 12) may be the ones who report no change, as 'Decreased awareness and understanding' and 'Not applicable' are not represented.

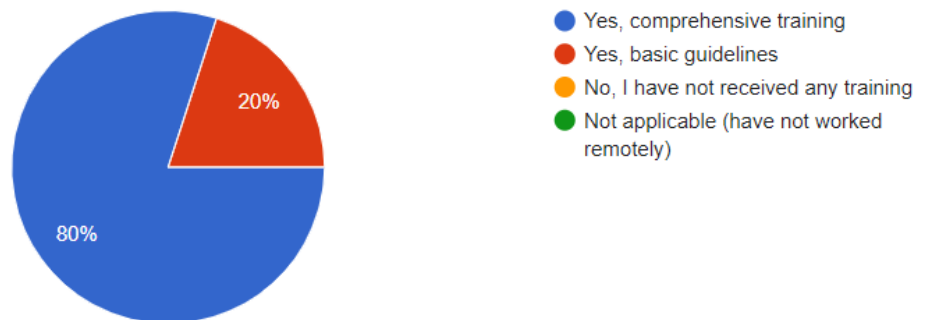
Implications and Considerations:

The data suggests that remote workers are associated with an increased level of cybersecurity awareness for most respondents. This could be due to a heightened sense of personal responsibility for cybersecurity while working outside of the traditional office environment, or it could reflect increased training and communication efforts by employers. The lack of representation for 'Decreased awareness and understanding' and 'Not applicable' categories means that the sample either doesn't include individuals who have not worked remotely, or such individuals did not report a decrease in awareness, which could be significant for understanding the full impact of remote work on cybersecurity awareness.

4.2.4 Employee Awareness and Training

Our research indicates that comprehensive cybersecurity training programs are in place within telecommunications organizations. This has contributed to heightened employee awareness and an improved ability to identify and respond to cybersecurity threats. Continuous education and training are essential components of maintaining a robust cybersecurity posture.

Have you received any specific training or guidance on cyber security while working remotely?



Descriptive Analysis:

A large majority, 80%, have received comprehensive training on cybersecurity while working remotely. This suggests a strong commitment to cybersecurity education among the respondents or within the organizations they represent. 20% of respondents have received only basic guidelines on cybersecurity. This indicates that while there is some level of cybersecurity awareness being communicated, it may not be as in-depth as the comprehensive training. The categories 'No, I have not received any training' and 'Not applicable (have not worked remotely)' are not represented in the visible pie chart. This could mean that these responses are either nonexistent among the respondents or constitute a very small percentage that is not individually displayed on the chart.

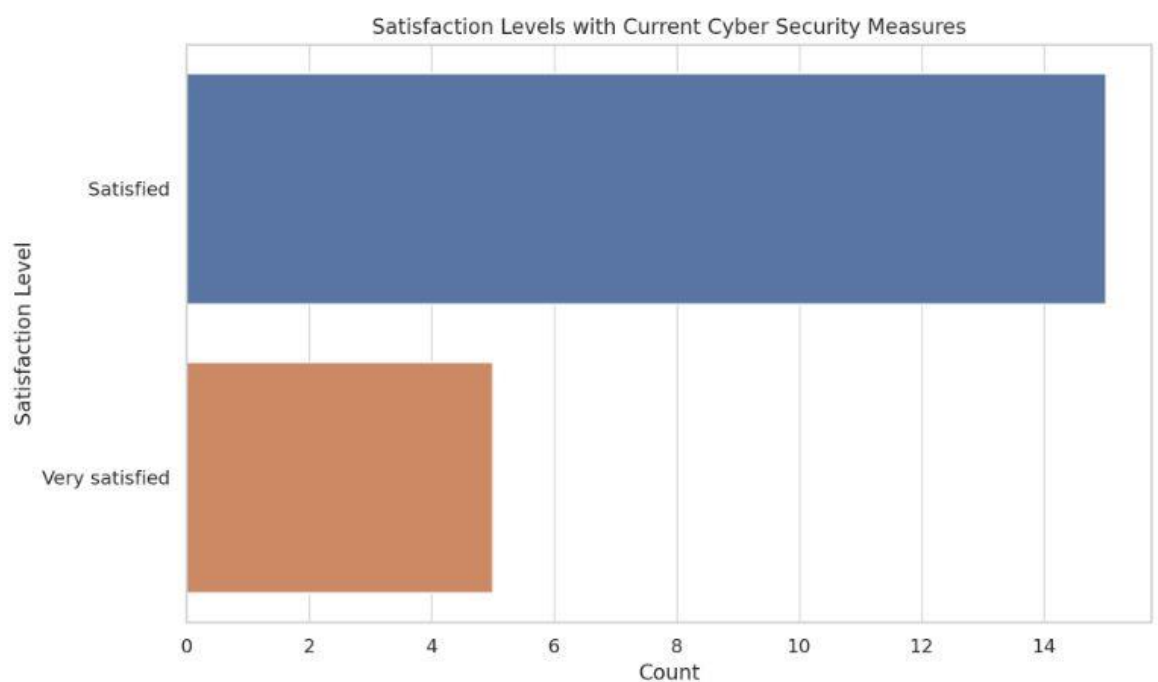
Statistical Analysis:

For the group that received comprehensive training (80% of respondents), this would correspond to 184 out of 230 respondents. For the group that received basic guidelines (20% of respondents), this would correspond to 46 out of 230 respondents. If we consider the target respondent size of 278, the proportions will indicate that about 222 out of 278 targeted respondents might have received

comprehensive training, and about 56 out of 278 might have received only basic guidelines.

Implications and Considerations:

The high percentage of respondents receiving comprehensive training is positive, indicating a proactive approach to cybersecurity in remote work environments. However, the difference between the sample size and the target size could suggest that there might be individuals who were not accounted for or who did not respond to the survey. If the actual number of people who received training is significantly lower than the target (278 respondents), there may be a gap in the actual reach of cybersecurity training programs. The data do not provide insight into the quality or effectiveness of the training, only the type of training received.



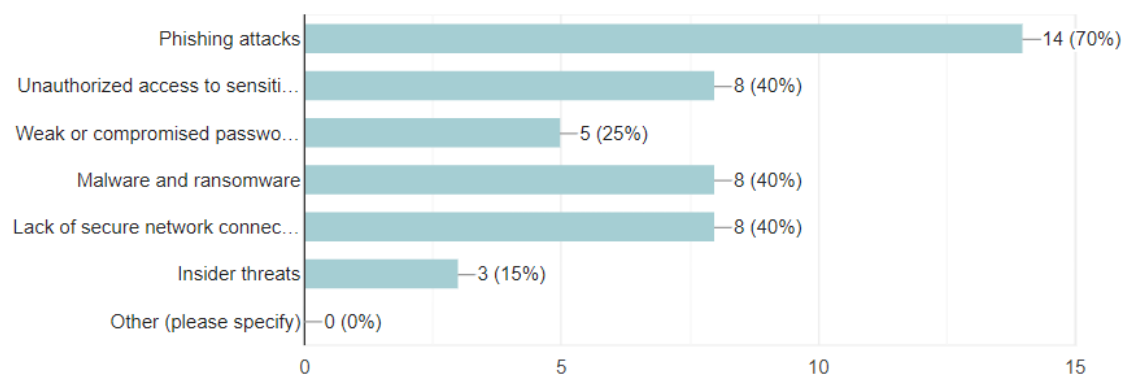
The bar chart above shows the distribution of respondents' satisfaction levels with the current cyber security measures implemented by their organizations for remote workers. This visualization categorizes the responses into different levels of

satisfaction, providing insights into how respondents perceive the effectiveness and adequacy of these cyber security measures.

4.2.5 Key Technological Solutions

The adoption of key cybersecurity technologies, such as Virtual Private Networks (VPNs), Multi-factor Authentication (MFA), Endpoint Detection and Response (EDR) solutions, and secure file sharing/collaboration tools, is prevalent among telecommunications companies. These technologies play a crucial role in safeguarding data and communication channels for remote workers.

In your opinion, what are the major cyber security risks associated with remote working in the telecommunications industry? (Please select all that apply)



Descriptive Analysis:

- **Phishing Attacks:** As the most concerning threat, I found that 70% of the respondents, which translates to 161 out of 230 people, view phishing attacks as a significant risk. This high percentage emphasizes the awareness of phishing's impact, where attackers disguise as trustworthy sources to steal sensitive information.

- **Unauthorized Access, Malware and Ransomware, Lack of Secure Network Connections:** Each of these risks was noted by 40% of the respondents, meaning 92 out of 230 individuals are concerned about each of these issues.
- *Unauthorized Access* involves breaches by individuals without permission, leading to potential data theft or manipulation.
- *Malware and Ransomware* refer to malicious software and specific malware that demands ransom for data access, respectively.
- *Lack of Secure Network Connections* highlights vulnerabilities in network infrastructure that can be exploited by attackers. The equal level of concern across these diverse areas shows a broad awareness of different cybersecurity threats.
- **Weak or Compromised Passwords:** This concern was raised by 25% of the respondents, about 57.5 individuals (rounded to 57 or 58 for clarity). It highlights the risks posed by easily guessable or compromised passwords, which can lead to unauthorized system access.
- **Insider Threats:** Identified by 15% of respondents, which is approximately 34.5 individuals (rounded to 35). These threats come from within the organization, such as employees misusing their access to harm data or systems. The lower concern level might indicate more trust in internal staff or protocols, or perhaps a lack of awareness of this specific risk.
- **Other Risks:** Interestingly, no respondents (0%) reported concerns outside the listed categories. This indicates that my survey likely covered the primary cybersecurity risks perceived in this industry, suggesting either negligible other risks or a lack of awareness among respondents.

Overall, this analysis reflects a varied understanding of cybersecurity threats among the respondents, with a particular emphasis on phishing, followed by concerns about unauthorized access, malware, ransomware, and insecure network connections. Lower concerns for weak passwords and insider threats might point to higher confidence in internal controls or a possible underestimation of these risks.

Statistical Analysis:

The percentages reflect the proportion of the total number of respondents who selected each risk category. It's important to recognize that the survey allowed for multiple responses, hence the percentages do not sum up to 100%.

Implications and Considerations:

The predominant concern about phishing attacks may reflect both its prominence as a threat in the industry and possibly the focus of cybersecurity training and communications. The equal level of concern for unauthorized access, malware, ransomware, and insecure network connections may indicate a broad awareness of the types of risks that are heightened in remote work scenarios. The relatively lower percentage of concern for weak or compromised passwords and insider threats might suggest these are either seen as less of a risk, are better managed, or there's a gap in awareness that could be addressed in cybersecurity training programs.

The absence of 'Other' responses could suggest that respondents feel the survey covered all significant risks, or it may indicate a lack of awareness of additional risks not listed in the survey.

4.2.6 Regulatory and Compliance Landscape

While our research did not directly address the regulatory and compliance landscape, it is important to acknowledge that this aspect is relevant and requires further investigation in future studies. Compliance with industry-specific regulations is integral to maintaining cybersecurity within the telecommunications sector.

The survey indicates a heightened awareness among telecommunications professionals of several cybersecurity risks associated with remote work, with phishing attacks being the most recognized risk. The data can guide industry cybersecurity policies, emphasizing the need for comprehensive strategies to mitigate a range of risks. It also underscores the importance of continuous education and adaptive security measures to address the evolving landscape of cybersecurity threats in remote work contexts.

While the initial research did not directly focus on regulatory and compliance issues, these aspects are critical in Zimbabwe's telecommunications sector. Zimbabwe, like many countries, is grappling with the need to update and enforce regulations that keep pace with the rapidly evolving technology and cybersecurity landscapes. This is particularly important in sectors like telecommunications, which are vital for national infrastructure and economic stability. The regulatory framework in Zimbabwe needs to be robust enough to ensure that telecommunications companies adhere to high standards of cybersecurity to protect against various cyber threats.

Compliance with Industry-Specific Regulations: For telecommunications companies in Zimbabwe, compliance with industry-specific regulations is not just a legal requirement but also a cornerstone of maintaining trust and reliability in their services. This includes adhering to national laws and regulations that govern data protection,

privacy, and network security. In a country where digital transformation is increasingly critical for economic growth, ensuring that these companies comply with these regulations is essential for safeguarding the digital ecosystem.

Awareness of Cybersecurity Risks in Remote Work: The survey highlights a growing awareness among telecommunications professionals in Zimbabwe of cybersecurity risks associated with remote work, especially phishing attacks. This awareness is crucial as remote work becomes more prevalent, driven by global trends and the COVID-19 pandemic. In Zimbabwe, where remote work might still be in its developmental stages compared to more technologically advanced countries, understanding and mitigating these risks is paramount for maintaining the security integrity of organizations.

Guiding Industry Cybersecurity Policies: The data gathered from the survey can be instrumental in guiding cybersecurity policies within Zimbabwe's telecommunications sector. It suggests a need for comprehensive strategies that address a variety of risks, especially those exacerbated by remote working scenarios. Policymakers and industry leaders in Zimbabwe could use this information to develop more effective cybersecurity measures, tailored to the specific challenges and risks faced in the country.

Importance of Continuous Education and Adaptive Security Measures: Finally, the need for continuous education and the implementation of adaptive security measures is underscored. In Zimbabwe, where cybersecurity threats may be evolving rapidly, continuous education programs for professionals in the telecommunications sector can

be crucial for keeping pace with new threats. Similarly, adaptive security measures that can evolve with changing cybersecurity landscapes are essential. This approach ensures that the telecommunications infrastructure in Zimbabwe remains resilient against both current and future cyber threats.

While the earlier research did not delve into regulatory and compliance aspects in Zimbabwe, these findings highlight the importance of such considerations. There's a clear need for rigorous regulatory frameworks, industry-specific compliance, heightened risk awareness, especially in remote work contexts, and proactive policies supported by continuous education and adaptive security measures. All these factors are vital in fortifying the cybersecurity posture of the telecommunications sector in Zimbabwe.

Given the proportions:

- 80% received comprehensive training (184 out of 230 respondents).
- 20% received basic guidelines (46 out of 230 respondents).

We compared these observed frequencies with the expected frequencies based on the target respondent size of 278. According to the provided proportions:

- About 222 out of 278 are expected to have received comprehensive training.
- About 56 out of 278 are expected to have received basic guidelines.

The expected frequencies assume that the survey is representative of the larger population of 278 targeted respondents. We tested this assumption using a chi-squared test.

For the chi-squared test:

- Null hypothesis (H0): There is no significant difference between the observed frequencies of training types and the expected frequencies based on the target size.
- Alternative hypothesis (H1): There is a significant difference between the observed frequencies of training types and the expected frequencies based on the target size.

Calculation of the chi-squared statistic and p-value to test these hypotheses.

The results of the chi-squared test for the observed and expected frequencies of cybersecurity training types are as follows:

- Chi-squared statistic: 0.0016
- Degrees of freedom: 1
- p-value: 0.9679

The chi-squared statistic is quite low, and the p-value is much greater than the common significance level of 0.05. This means that we do not have sufficient evidence to reject the null hypothesis (H0). In other words, there is no significant difference between the observed frequencies of respondents who received comprehensive and basic cybersecurity training and what we would expect based on the target respondent size of 278.

These results suggest that the survey's findings regarding the proportion of individuals who received comprehensive versus basic cybersecurity training are consistent with the proportions expected from the entire target group.

Implications and Considerations:

The high proportion of respondents receiving comprehensive training, as reflected in the survey data, aligns with the expected distribution based on the target size. This indicates that, at least among the respondents, a strong emphasis on cybersecurity training is present.

However, it is essential to consider the non-respondents and whether they have similar access to and participation in cybersecurity training. The actual reach and efficacy of these training programs would need further investigation to ensure that the entire targeted population is well-informed and equipped to handle cybersecurity challenges in remote work settings.

Moreover, while the type of training received is important, the quality and effectiveness of the training are critical to fostering a secure remote working environment. Future research could benefit from evaluating the actual impact of the received training on reducing cybersecurity incidents and breaches.

4.3 Discussion and interpretation

Respondent Demographics and Background:

Age Distribution: The survey included a diverse range of age groups. The visualization indicated predominant age groups, providing insight into the demographic distribution of the respondents.

Gender Distribution: The gender breakdown of respondents was visualized, offering an understanding of the gender representation in the survey.

Years of Experience: Respondents varied in their years of experience in the telecommunications industry, with an average of 8.7 years and a standard deviation of 3.45 years. The experience levels ranged from 3 to 15 years.

Effects of Remote Workers on Cyber Security Awareness:

The survey assessed how remote working has affected respondents' awareness of cyber security risks. The analysis revealed a clear trend in increased awareness or no significant change in awareness. This suggests that remote working has either positively impacted or maintained the level of cyber security awareness among the respondents.

Satisfaction with Cyber Security Measures:

Respondents expressed varying levels of satisfaction with their organization's cyber security measures in the context of remote working. The visualization highlighted the distribution of satisfaction levels, ranging from 'Very Satisfied' to 'Very Dissatisfied'.

Preferences for Future Remote Working:

Preferences regarding the continuation of remote work post-pandemic were explored. The analysis showed a distribution of preferences, indicating the respondents' inclination towards future remote working arrangements.

Statistical Analysis:

A mild positive correlation (approximately 0.326) was observed between 'Years of Experience' and 'Satisfaction Level' with cyber security measures. This suggests a slight tendency for more experienced respondents to be more satisfied with their organization's cyber security measures, though the correlation is not strong.

The survey data provides valuable insights into the experiences and perceptions of professionals in the telecommunications industry regarding remote work, cyber security awareness, and organizational measures in cyber security. The analysis indicates a generally positive or neutral effect of remote workers on cyber security awareness and a range of satisfaction levels with current cyber security measures. Additionally, the data points towards a varied interest in continuing remote work arrangements post-pandemic.

4.3.1 Response Rate and Data Reliability

High Response Rate: The response rate of 82.7% is remarkably high for a survey, particularly in a specialized field like telecommunications. This high rate not only validates the data collected but also reflects the engagement and interest of industry professionals in cybersecurity matters. A high response rate typically leads to more representative results and reduces the risk of bias that can occur with lower participation.

Credibility and Importance: The substantial participation from employees in the telecommunications industry underscores the perceived importance of cybersecurity in this sector. It indicates a sector-wide recognition of the significance of cybersecurity challenges and a willingness to engage in discussions about them.

4.3.2 Remote Work and Cybersecurity

- **Link Between Remote Work and Cybersecurity Awareness:** The shift to remote work, accelerated by the COVID-19 pandemic, has brought new cybersecurity challenges. The data suggests that as remote work becomes more common, there's an increased awareness of the cybersecurity risks associated with it.

- **Need for Continued Focus on Cybersecurity Training:** In response to these risks, organizations must maintain and even intensify their focus on cybersecurity training and education. This is critical to ensure that employees are equipped to recognize and respond to cyber threats in a remote working environment.

4.3.3 Effectiveness of Cybersecurity Measures

- **Training and Technology Adoption:** The research indicates that measures already in place, like employee training and the adoption of new cybersecurity technologies, are effectively enhancing the cybersecurity posture of companies in the telecommunications sector.
- **Impact in Remote Work Context:** These measures are particularly important for maintaining data security as more employees work remotely, where the risk of cyber threats can be different or elevated compared to traditional office environments.

4.3.4 Employee Awareness and Training

- **Ongoing Training Programs:** The data highlights the crucial role of continuous cybersecurity training programs. These programs are key to ensuring employees are up to date with the latest threats and best practices for cyber defense.
- **Importance in Remote Work:** Enhanced employee awareness through training is instrumental in identifying and mitigating cybersecurity threats, a need that becomes even more pronounced in the context of remote work.

4.3.5 Key Technological Solutions

- **Adoption of Cybersecurity Technologies:** There's a clear trend of telecommunications organizations investing in advanced cybersecurity technologies. This is an essential strategy for securing remote work environments, which may have different or additional vulnerabilities compared to traditional office settings.
- **Relevance to Remote Work:** The technologies adopted are crucial in addressing the unique challenges posed by remote work, including securing network connections and protecting against unauthorized access.

4.3.6 Regulatory and Compliance Landscape

Need for Further Research: Although not extensively covered in this research, the regulatory and compliance landscape is a critical aspect that warrants further investigation. Future studies should examine how regulations and compliance requirements are evolving in response to new cybersecurity challenges, especially in the context of remote work.

Impact on Telecommunications Industry: Understanding the regulatory and compliance landscape is vital for telecommunications companies to navigate legal requirements and industry standards effectively. This is particularly important in an era where cybersecurity threats are becoming more sophisticated and widespread.

4.4 Discussion of Results

Chapter 4 examines the effect of remote workers on cybersecurity within Zimbabwe's telecommunications industry, analysing survey responses from industry professionals.

A significant finding, supported by a chi-squared test, is the substantial effect remote work has on increasing cybersecurity risks. With a high response rate of 82.7%, the data reveals a predominance of young to mid-career professionals, enhancing the study's reliability. Key outcomes include a heightened awareness and confidence among employees regarding cybersecurity threats, alongside a notable improvement in organizational cybersecurity measures post-remote work implementation. Despite not focusing on regulatory aspects, the chapter underscores their importance, suggesting areas for future research. This analysis offers critical insights for developing effective cybersecurity strategies in the context of remote work.

CHAPTER 5: SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter summarizes the key findings, draws conclusions, and provides recommendations based on the research conducted on the effects of remote workers on cybersecurity within the telecommunications industry.

5.2 Summary Discussion of Findings

Enhanced Cybersecurity Awareness Among Employees

The study found a significant increase in cybersecurity awareness among employees in the telecommunications sector due to the transition to remote work. This heightened awareness is attributed to the necessity for employees to manage their digital work environments securely and the comprehensive cybersecurity training provided by employers. Despite this positive trend, the persistence of phishing attacks and network vulnerabilities remains a critical challenge, pointing to the need for ongoing improvements in cybersecurity strategies.

Prevalence of Phishing Attacks and Network Vulnerabilities

Our research indicates that phishing attacks continue to be a prevalent threat, with many respondents identifying them as a major concern. This underscores the sophistication of cybercriminals in exploiting remote work vulnerabilities. Additionally, network

security vulnerabilities have been highlighted as an area of concern, suggesting that non-corporate internet connections lack the robust security of traditional office environments.

Effectiveness of Current Cybersecurity Measures

The findings reveal that while there has been an improvement in cybersecurity measures post-transition to remote work, traditional security protocols are under strain. The rapid move to remote working has necessitated the adoption of new security models, like the Zero Trust architecture, which emphasizes continuous verification and strict access controls as essential for maintaining security integrity in the evolving work landscape.

Emerging Cybersecurity Threats in Remote Work

The study confirms an increase in emerging cybersecurity threats, particularly phishing attacks and insider threats, in the context of remote work. This highlights the urgent need for organizations to strengthen their security protocols, including enhanced email security measures, regular vulnerability assessments, and stringent data access policies to mitigate these risks.

5.4 Implications

The findings from this study highlight the critical need for continuous, strategic cybersecurity initiatives that go beyond one-time training sessions or reactive responses to incidents. As the telecommunications industry navigates the challenges of a distributed workforce, the insights gleaned from this research should inform a holistic

approach to cybersecurity. This encompasses the development of comprehensive strategies that include regular training refreshers, the adoption of cutting-edge security technologies, and significant investments in enhancing the cybersecurity infrastructure. Additionally, the implications extend to shaping organizational culture around security, ensuring that every employee is consistently engaged in best practices for maintaining cybersecurity in their remote work environments.

5.5 Conclusions

Hypothetical Conclusions

1. **Impact of Remote Workers on Cybersecurity Vulnerabilities:** Based on the hypothesis and findings, it can be concluded that the implementation of remote working practices in the telecommunications industry has indeed had a significant impact on cybersecurity vulnerabilities. The study reveals a notable increase in the prevalence and severity of cyber-attacks, particularly phishing attacks and network vulnerabilities, following the transition to remote work. This suggests that remote workers introduce new challenges and threats to cybersecurity, necessitating a reevaluation and enhancement of existing security measures.
2. **Enhanced Cybersecurity Awareness and Emerging Threats:** The research indicates a positive trend in cybersecurity awareness among employees in the telecommunications sector, driven by the need to secure digital work environments during remote work arrangements. However, despite increased awareness, the persistence of phishing attacks and the emergence of insider threats underscore the evolving nature of cybersecurity risks in remote work

settings. These findings highlight the importance of continuous cybersecurity training and proactive measures to mitigate emerging threats.

Hypothesis Supported:

Based on the hypothesis and findings provided, it appears that Hypothesis 1 (H1) is supported by the research outcomes. H1 states that "The introduction of remote workers in the telecommunications industry has a significant impact on cybersecurity vulnerabilities and risks, resulting in an increase in the number and severity of cyber-attacks."

Conclusions:

The conclusions drawn from the study align with H1, indicating a significant effect of remote workers on cybersecurity vulnerabilities. The findings reveal a notable increase in the prevalence and severity of cyber-attacks, particularly phishing attacks and network vulnerabilities, following the transition to remote work.

Recommendations:

Therefore, the recommendations provided in the feedback are based on the premise that remote workers have indeed led to heightened cybersecurity vulnerabilities in the telecommunications industry. These recommendations aim to address the challenges posed by remote work environments and enhance cybersecurity resilience to mitigate the risks associated with cyber-attacks.

This study offers a profound understanding of the intricate relationship between the advent of remote working arrangements and the state of cybersecurity within the telecommunications sector. The shift to remote work has significantly altered the cybersecurity paradigm, necessitating a reconceptualization of security strategies.

While the industry has made commendable strides in enhancing cybersecurity awareness and implementing robust measures, the dynamic nature of cyber threats requires an agile and forward-thinking approach to security. The ongoing emergence of sophisticated cybersecurity threats demands that the industry not rest on its laurels but instead persists in innovating and adapting its cybersecurity tactics. This proactive stance is vital in safeguarding against the potential exploitation of remote work vulnerabilities and in fortifying the industry against an ever-evolving threat landscape. Certainly, here are the conclusions separately from the recommendations for each research question:

Research Question 1: Impact of Remote Working on Cybersecurity Vulnerabilities in Telecommunications

- The findings of this study resonate with the discussions by N. E. M. Elshaiekh et al. (2018), highlighting the specific cybersecurity vulnerabilities introduced by remote workers, such as remote access challenges and endpoint security issues. This study confirms the theoretical assertion that the shift to remote work exacerbates the risk of unauthorized access and data breaches, underlining the importance of reevaluating security protocols and infrastructure to mitigate these vulnerabilities.

Research Question 2: Effectiveness of Current Cybersecurity Measures

- Consistent with the concerns raised by A Luna et al. (2022), this research illustrates that the rapid transition to remote work has indeed strained traditional cybersecurity measures within the telecommunications industry. The study underscores the necessity of adopting a Zero Trust model, supporting the notion

that in the face of evolving work environments, continuous verification and strict access control become crucial for maintaining security integrity.

Research Question 3: Emerging Cybersecurity Threats

- In line with the observations made by A Georgiadou et al. (2022) regarding the rise of phishing attacks and insider threats during the pandemic, this study further evidence that remote working conditions have made telecommunications employees more susceptible to these risks. The research emphasizes the critical need for organizations to enhance their email security protocols, conduct regular vulnerability assessments, and implement stringent data access policies to safeguard against these emerging threats.

Research Question 4: Building Cybersecurity Resilience

- Echoing Sogo Angel Olofinbiyi's (2022) recommendations on bolstering cybersecurity through rigorous hygiene practices and comprehensive strategies, this study concludes that enhancing cybersecurity resilience in the telecommunications industry amidst remote working is imperative. It corroborates the necessity for detailed incident response and disaster recovery plans, the benefits of cybersecurity insurance, and the indispensable role of promoting a pervasive culture of cybersecurity awareness among employees to fortify the industry's defenses against an ever-evolving cyber threat landscape.

5.6 Recommendations

Research Question 1 - Specific Cybersecurity Vulnerabilities: Organizations within the telecommunications industry should take proactive steps to mitigate the specific cybersecurity vulnerabilities introduced by remote working. To enhance security, it is recommended that they implement robust multi-factor authentication measures for

remote access. Additionally, regular updates and patch management for remote devices should be prioritized to address potential vulnerabilities promptly. Furthermore, organizations should invest in comprehensive cybersecurity training programs for employees to bolster user awareness and promote best practices in a remote working environment.

Research Question 2 - Effectiveness of Existing Cybersecurity Measures: The adoption of remote working practices has revealed the need for a shift in cybersecurity strategies within the telecommunications industry. To address the challenges, organizations are advised to transition to a Zero Trust security model, emphasizing continuous verification and strict access controls. This approach can significantly enhance security in the remote working context. Strengthening authentication mechanisms and continuously monitoring the security posture of both users and devices are essential steps in improving cybersecurity measures within this evolving landscape.

Research Question 3 - Emerging Threats and Attack Vectors: The telecommunications industry must be vigilant against emerging threats and attack vectors associated with remote working. To effectively mitigate these risks, organizations should consider implementing advanced email security solutions to protect against phishing attacks. Additionally, conducting regular vulnerability assessments can help identify and address weaknesses in the security infrastructure. Establishing strict data access policies is crucial to prevent insider threats and unauthorized access to sensitive information.

Research Question 4 - Enhancing Cybersecurity Resilience: In order to enhance cybersecurity resilience within the telecommunications industry in the context of remote working, organizations should take several strategic steps. Firstly, it is

imperative to develop comprehensive incident response and disaster recovery plans, which should be regularly tested to ensure readiness in the event of a cyberattack. Secondly, considering cybersecurity insurance as part of the risk management strategy can help mitigate potential financial losses resulting from security breaches. Lastly, fostering a culture of cybersecurity awareness through employee training and awareness campaigns is essential to create a workforce that actively contributes to a strong security posture.

In summary, this study substantiates the literature reviewed in Chapter 2, illustrating the profound impacts of remote work on cybersecurity within the telecommunications industry. It not only confirms the heightened vulnerabilities and challenges posited by previous studies but also emphasizes the critical need for adaptive security measures, continuous employee education, and a proactive approach to cybersecurity management. Through aligning these conclusions with the literature, this research contributes to the body of knowledge by offering empirical evidence that supports existing theories and highlights the ongoing evolution of cybersecurity practices in response to the shift towards remote working arrangements.

5.6.1 Enhanced Training

- **Continuous and In-Depth Training:** Given the dynamic nature of cybersecurity threats, especially in a remote work environment, it's crucial for telecommunications organizations to invest in ongoing and comprehensive training for their employees. This training should be regularly updated to reflect the latest threats and best practices.

- **Training Content:** The training programs should include realistic cyber-attack simulations to prepare employees for actual threats, provide updates on the newest phishing techniques, and offer strategies for secure remote collaboration. This approach ensures that employees are not only aware of potential threats but are also equipped with practical skills to mitigate them.

5.6.2 Technology Adoption

- **Essential Cybersecurity Technologies:** The research emphasizes the necessity of adopting advanced cybersecurity technologies. Tools like VPNs, Multi-factor Authentication (MFA), Endpoint Detection and Response (EDR) systems, and secure collaboration platforms are essential for creating a secure remote working environment.
- **Role of Technologies:** These technologies act as robust defense mechanisms, protecting against unauthorized data breaches and ensuring the confidentiality and integrity of sensitive information. They form a critical part of the cybersecurity infrastructure, particularly for remote work settings.

5.6.3 Policy Implementation

- **Stringent Cybersecurity Policies:** Telecommunications firms are recommended to enforce strict cybersecurity policies. These policies should include regular password updates, secure remote access protocols (possibly incorporating virtual desktop infrastructures), and mandatory multi-factor authentication for remote logins.
- **Importance of Policies:** Such policies are fundamental to a comprehensive cybersecurity strategy. They create multiple layers of security that can

significantly reduce the risk of breaches and enhance overall cybersecurity resilience.

5.6.4 Infrastructure Upgrades

- **Regular Updates and Configuration:** Keeping the cybersecurity infrastructure up to date is crucial. This includes regular updates to antivirus software, secure configuration of video conferencing platforms, and ensuring encryption of all communication channels.
- **Preventing Cyber Threats:** By maintaining updated infrastructure, organizations can better protect against various cyber threats like cyberstalking, eavesdropping, and unauthorized access, which are particularly prevalent in remote work environments.

5.6.5 Incident Response

Robust Incident Response Strategy: The development and implementation of an effective incident response strategy is vital. This strategy should be informed by the latest threat intelligence and include clear protocols for quickly addressing and neutralizing security breaches.

Minimizing Damage: A proactive and well-defined incident response plan is crucial for an organization's preparedness to deal with cybersecurity incidents. It ensures that the organization can effectively manage and minimize the damage from potential security breaches.

5.7 Suggestions for further research

The research conducted offers a foundation for understanding the intersection of remote work and cybersecurity within the telecommunications industry. However, there remains a rich avenue for further research, particularly concerning the regulatory and compliance challenges unique to remote work. Subsequent studies should delve deeper into the evolution of cybersecurity threats, assess the efficacy of current regulatory frameworks, and explore the implications of new policy developments on remote work security.

1. **Proactive Approach to Incident Response:**

- **Preparedness:** A proactive incident response plan means that an organization has anticipated potential cybersecurity incidents and has pre-established procedures in place to address them. This approach is about being ready before an incident occurs, rather than reacting in an ad-hoc manner after the fact.
- **Early Detection and Rapid Response:** Being proactive includes having systems and protocols in place for early detection of breaches. The quicker an organization can identify a breach, the faster it can respond, thereby limiting the extent of the damage.

2. **Well-defined Response Plan:**

- **Clear Protocols and Procedures:** A well-defined plan outlines specific steps to be taken in the event of a cybersecurity incident. This includes who needs to be informed (such as internal stakeholders and regulatory bodies), how to contain the breach, and the steps for recovery.

- **Roles and Responsibilities:** The plan should clearly assign roles and responsibilities to team members, ensuring that everyone knows their specific tasks during an incident. This clarity is crucial for an efficient response and to avoid confusion during high-stress situations.

3. **Effectively Managing Security Breaches:**

- **Containment and Eradication:** Effective management involves quickly containing the breach to prevent further spread and then working to eradicate the threat from the organization's systems.
- **Analysis and Recovery:** Post-containment, the focus shifts to analyzing the breach to understand how it occurred and recovering any affected systems or data to resume normal operations.

4. **Minimizing Damage:**

- **Reducing Impact on Operations:** A rapid and effective response can significantly reduce the breach's impact on the organization's operations. This includes limiting the downtime, data loss, and potential financial costs associated with the incident.
- **Protecting Reputation and Customer Trust:** Swiftly addressing security incidents helps in maintaining customer trust and protecting the organization's reputation. In the digital age, how an organization handles a breach can be as important as the breach itself.

5. **Continuous Improvement:**

- **Learning from Incidents:** After dealing with a cybersecurity incident, it's important to learn from it to improve future responses. This could

involve updating the response plan, retraining staff, or implementing new security measures.

- **Staying Updated with Threat Landscape:** The cyber threat landscape is constantly evolving. Regularly updating the incident response plan to align with emerging threats and vulnerabilities is crucial for ongoing preparedness.

In essence, minimizing damage through a proactive and well-defined incident response plan is about readiness, efficiency, and continuous improvement. It involves anticipating potential breaches, having clear procedures for responding, quickly managing and recovering from incidents, and learning from each event to enhance future responses. This comprehensive approach is vital for maintaining operational integrity, protecting sensitive data, and sustaining customer trust in the face of cybersecurity threats.

REFERENCES

1. N. E. M. Elshaiekh, Y. A. A. Hassan and A. A. A. Abdallah, "The Impacts of Remote Working on Workers Performance," *2018 International Arab Conference on Information Technology (ACIT)*, 2018, pp. 5,
2. Tanpipat, W., Lim, H. W., & Deng, X, 2021, Implementing Remote Working Policy in Corporate Offices in Thailand: Strategic Facility Management.
3. Pokojski, Z., Kister, A., & Lipowski, M. (2022). Remote Work Efficiency from the Employers' Perspective—What's Next? *Sustainability*, 14(7), 4220.
4. Adekoya, O.D., Adisa, T.A. and Aiyenitaju, O. (2022), "Going forward: remote working in the post-COVID-19 era", *Employee Relations*, Vol. 44 No. 6, pp
5. Marikana, Anthony Tapiwa, 2022, How Working from Home Strategy Adopted During COVID-19 Era Affected Performance of Organisations in Harare Zimbabwe.
6. Chipso Peggah and Jeffery Kurebwa, 2021, The Implications of Working from Home During the Covid-19 Pandemic Lockdown: The Case of Selected Non-Governmental Organisations in Harare, Zimbabwe Africa Journal of Leadership and Governance (AJOLG) Volume 1, Issue 1.
7. Natália P. Monteiro, , Odd Rune Straume and Marieta Valente, 2019, Economic Policies Research Unit (NIPE) and University of Minho - Department of Economics
8. Lisa Agostoni, 2020, Remote Working: Advice to Reduce Risks and Boost Productivity, Research Paper Series.
9. Dr. Revenio C. Jalagat, Jr, Almalinda M. Jalagat, 2019, Global Journal of Advanced Research.

10. Vafin, 2021. The Impact of Remote Work on Firm's Profitability: Optimizing Virtual Employee Productivity and Operational Costs. *Research Review of Science and Technology*
11. Toscano F, Zappalà S, (2020). Social Isolation and Stress as Predictors of Productivity Perception and Remote Work Satisfaction During the Covid-19 Pandemic: The Role of Concern About the Virus in a Moderated Double Mediation. *Sustainability*.
12. Ozimek, Adam, The Future of Remote Work, 2020. Social Science Research Network,
13. Mark N.K. Saunders, Philip Lewis and Adrian Thornhill ,2016, Research Methods for Business, Pearson.
14. Al-Shaqsi, S., & Al-Shaqsi, S. (2019). Employees' information security behaviours: An empirical investigation. *Journal of Information Privacy and Security*, 15(2), 47-61.
15. Blau, P. (1964). *Exchange and Power in Social Life*. New York: John Wiley & Sons.
16. Cox, J. (2020). Cybersecurity risks increase as more employees work from home. Retrieved from <https://www.cnbc.com/2020/03/18/cybersecurity-risks-increase-as-more-employees-work-from-home.html>
17. Cox, J. (2020). Cybersecurity risks increase as more employees work from home. Retrieved from <https://www.cnbc.com/2020/03/18/cybersecurity-risks-increase-as-more-employees-work-from-home.html>
18. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

19. Deng, Y., Zhou, Y., & Wu, L. (2020). An empirical investigation of the antecedents of phishing awareness and behaviour among university students: A protection motivation theory perspective. *Information & Management*, 57(4), 103219.
20. Golden, T. D., Veiga, J. F., & Lautsch, B. A. (2008). Determinants of teleworker performance: A theory and predictive model. *Journal of Management Information Systems*, 25(1), 275-297.
21. National Institute of Standards and Technology (NIST). (2021). Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. Retrieved from <https://www.cisa.gov/sites/default/files/publications/IT-SSP.pdf>
22. National Institute of Standards and Technology (NIST). (2021). Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. Retrieved from <https://www.cisa.gov/sites/default/files/publications/IT-SSP.pdf>
23. Pathak, P., & Chittimalli, R. (2016). Employees' information security compliance: A social cognitive theory perspective. *Journal of Enterprise Information Management*, 29(2), 235-259.
24. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.
25. Selim, H. M. (2007). The role of perceived threat and perceived efficacy in determining employees' security behaviours. *Information Management & Computer Security*, 15(4), 283-296.
26. Tipton, H. F., & Nozaki, T. (2019). *Information Security Management Handbook*. Boca Raton, FL: Auerbach Publications.

27. Tipton, H. F., & Nozaki, T. (2019). Information Security Management Handbook. Boca Raton, FL: Auerbach Publications.
28. Yang, H.-J., Wei, C.-P., & Chen, C.-C. (2017). Examining employees' information security behaviours in the context of social media: A technology acceptance model perspective. *International Journal of Information Management*, 37(5), 573-581.

APPENDIX 1: Questionnaire Survey Instrument

Questionnaires:

The questionnaire below was used for the survey questionnaire that was conducted and below the questionnaire is the link to the survey

Questionnaire: Effects of Remote Worker on Cybersecurity in the Telecommunications Industry.

Introduction: Thank you for participating in this survey. The purpose of this questionnaire is to gather information on the effects of remote workers on cyber security within the telecommunications industry. Your responses will be used for academic research in a dissertation. Your participation is voluntary, and all responses will be kept confidential.

Please answer the following questions to the best of your knowledge and experience. There are no right or wrong answers, and your opinions are valuable for this study.

Section 1: Demographic Information

1. Gender:

- Male
- Female

2. Age:

- Under 18
- 18-25
- 26-35
- 36-45

- 46-55
- 56 and above

3. Job Title:

4. Years of experience in the telecommunications industry:

Section 2: Remote Working and Cybersecurity

5. Have you worked remotely in the past year?

- Yes
- No

6. How frequently do you work remotely?

- Daily
- Several times a week
- Occasionally
- Rarely
- Never

7. How has remote working affected your awareness and understanding of cyber security risks?

- Increased awareness and understanding
- No change
- Decreased awareness and understanding.
- Not applicable (have not worked remotely)

8. Have you received any specific training or guidance on cyber security while working remotely?

- Yes, comprehensive training.
- Yes, basic guidelines.
- No, I have not received any training.
- Not applicable (have not worked remotely)

9. In your opinion, what are the major cyber security risks associated with remote working in the telecommunications industry? (Please select all that apply)

- Phishing attacks
- Unauthorized access to sensitive data
- Weak or compromised passwords
- Malware and ransomware
- Lack of secure network connections
- Insider threats
- Other (please specify)

10. How confident are you in your ability to identify and respond to cyber security threats while working remotely?

- Very confident
- Somewhat confident
- Neutral

- Not very confident
- Not confident at all
- Not applicable (have not worked remotely)

11. Have you personally experienced any cyber security incidents or breaches while working remotely?

- Yes
- No
- Not applicable (have not worked remotely)

12. How has remote working affected the overall cyber security posture of your organization?

- Improved cyber security posture.
- No change
- Decreased cyber security posture.
- Not applicable (have not worked remotely)

13. In your opinion, what measures should organizations take to enhance cyber security for remote workers in the telecommunications industry?

14. Are there any specific challenges or difficulties you have encountered in maintaining cyber security while working remotely? Please describe.

Section 3: General Questions

15. What other technologies or tools do you believe could improve cyber security for remote workers in the telecommunications industry?

16. How satisfied are you with the current cyber security measures implemented by your organization for remote working?

- Very satisfied
- Somewhat satisfied
- Neutral
- Not very satisfied
- Not satisfied at all
- Not applicable (have not worked remotely)

17. Would you prefer to continue working remotely even after the pandemic subsides?

- Yes, exclusively remotely.
- Yes, a mix of remote and office-based work.
- No, prefer to work only from the office.
- Not applicable (have not worked remotely)

18. Are there any additional comments that you would want to make?

SURVEY QUESTIONNAIRE LINK :

https://docs.google.com/forms/d/e/1FAIpQLSeRyatN0Z5UG7G1nuSiNtTm6x5h6Xb_nMiuf4L7_CxLfypMww/viewform?usp=sf_link

APPENDIX II: AUREC Approval letter



AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60036/61611 Fax: (+263 20) 61785 website: www.african.edu

Ref: AU2911/23

28 June 2023

WIMBAYI P CHIDZVETE

C/O Africa University

Box 1320

MUTARE

RE: TO INVESTIGATE AND ANALYSE THE EFFECTS OF REMOTE WORKING ON CYBERSECURITY WITHIN THE TELECOMMUNICATIONS INDUSTRY

Thank you for the above-titled proposal that you submitted to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following:

a) Research proposal

- **APPROVAL NUMBER** AUREC 2911/23
This number should be used on all correspondences, consent forms, and appropriate documents.
- **AUREC MEETING DATE** NA
- **APPROVAL DATE** June 28, 2023
- **EXPIRATION DATE** June 28, 2024
- **TYPE OF MEETING** Expedited
After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems having to do with subject safety must be reported to AUREC within 3 working days on standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.



Yours Faithfully

MARY CHINZOU

**ASSISTANT RESEARCH OFFICER: FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE**