CYBERSECURITY AWARENESS STRATEGY FOR RURAL COMMUNITIES: A CASE STUDY OF THE MOPANI DISTRICT IN THE LIMPOPO PROVINCE

By

PHOLOSHO WISANI MASILANE

18019432

Submitted in Accordance with the Requirements for the Degree of Master of Commerce in Business Information Systems

in the Faculty of Management, Commerce and Law

at the University of Venda

Supervisor: Prof. A. Kadyamatimba.

Co-Supervisor: Dr. S. Madzvamuse.

2024

DECLARATION

I, Pholosho Wisani Masilane, declare that this research reported in this dissertation entitled **"Cybersecurity Awareness Strategy for Rural Communities: A Case Study of the Mopani District in the Limpopo Province"**, except where otherwise indicated, is my original work and is prepared in partial fulfilment of the requirements of the Degree of Master of Commerce in Business Information Systems at the University of Venda. I also declare that this dissertation has not been submitted at the University of Venda or at any other institution before and all sources I have used are fully acknowledged through complete citations and references.

Researcher's Signature:  **Date:** 06/05/2024

Researcher's Name: Pholosho Wisani Masilane

ACKNOLEDGEMENT

First and foremost, I would like to extend my profound gratitude to Almighty God for bestowing upon me the opportunity to complete this research study and for granting me the resilience necessary to persevere through its challenges. I deeply appreciate the unwavering support, encouragement, and invaluable guidance my parents, Philison and Samaria Masilane, and my family provided. Their steadfast presence and support during personal and spiritual adversity, including times of illness and moments when I contemplated withdrawing from my studies, served as a continuous source of inspiration and motivation throughout this journey.

I would also like to express my sincere appreciation to my supervisor, Prof. Armstrong Kadyamatimba, and co-supervisor, Dr. Solomon Madzvamuse, for their exceptional guidance and support throughout the research project. Their expertise and constructive feedback were instrumental in the successful completion of this study.

Additionally, I extend my heartfelt thanks to my close friend, Victoria Nkuna, and my dear companion, Mixo Origion Sibuyi, for their direct and indirect support and guidance. Their contributions were significant in achieving the successful completion of this research endeavor.

ABSTRACT

Cybersecurity challenges persist in rural communities, exacerbated by the lack of effective cybersecurity awareness strategies. This study aimed to address these challenges by developing a tailored cybersecurity awareness strategy specifically for rural communities in Limpopo Province, Mopani District. The research focused on identifying cybersecurity challenges, factors influencing cybersecurity policies, and assessing cybersecurity awareness and attitudes within these communities. Data was collected through random multi-stage sampling and referral techniques using a questionnaire. The findings revealed a significant prevalence of cyberattacks (81%), with phishing being the most common type. Consequences included data loss, stolen personal information, service disruptions, financial loss, and reputation damage. Key challenges identified encompassed limited awareness, restricted access to resources, weak policies, and insufficient training. The developed strategy focuses on enhancing training programs, improving resource accessibility, and strengthening policy frameworks, which together lay the groundwork for fostering a cybersecurity culture and mitigating cyber threats in rural communities.

Keywords: *Cybersecurity, Cyberattacks, Cybersecurity awareness, rural communities, Mopani district, Limpopo.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IT	Information Technology
ICT	Information and Communication Technology
CSIR	The Council for Scientific and Industrial Research
NGO	Non-governmental Organization
COBIT	Control Objectives for Information and Related Technology
NIST	National Institute of Standards and Technology
ITIL	Information Technology Infrastructure Library
APWG	Anti-Phishing Working Group
COVID-19	Coronavirus Disease of 2019
COSO	Committee of Sponsoring Organizations
ISO	International Organization for Standardization
ERM	Enterprise Risk Management
ISACA	Information Systems Audit and Control Association
FISMA	Federal Information Security Modernization Act
ENISA	European Union Agency for Cybersecurity
Gov	Government
APWG	Anti-Phishing Working Group
N	Number

1. CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1. Introduction and Background

Over the decade, the internet has significantly impacted our lives by shaping our economy and society through the development of extensive communications channels and networking infrastructure, satisfying individuals' needs for access to information from any location and at any time (Wekunda, Aduda, and Guyah, 2021). Connectivity and digital (online) storage are services which people are increasingly accustomed to, thanks to the development of smart low-cost devices (Mabaso and Kumar, 2018). These smart low-cost devices include the desktop PC, laptop, tablet, and smartphones (Mbamaluikem and Ogunyemi, 2022). The adoption of ICT services such as internet represents fundamentals of knowledge growth for individuals, businesses and countries that can exploit them. Furthermore, the influence of ICT continues to expand, offering opportunities to individuals that enable them to gain access to information (Baporikar, 2020). Hence, the use of ICT, including the internet, it is considered a crucial factor that enables businesses and individuals to simplify their daily lives.

The study focuses on the intersection of ICT and cybersecurity, particularly examining the development and implementation of cybersecurity awareness strategies within rural communities. By narrowing the scope to this specific area, the study aims to provide a cohesive analysis of how cybersecurity challenges are addressed in the context of increasing ICT usage in these communities.

According to Soomro, Kumar and Kumari, (2022), ICT has evolved over many years to its current level of accessibility and affordability, and it stands as one of the most crucial factors driving economic development in our globalised economy. The internet and its infrastructures are critical for governments, businesses, and individuals as a mode of communication (Halouzka, Kozak, Buřita, and Matoulek, 2021). The means of communication available to humanity now are more efficient and effective than those which were previously available. Soomro et al. (2022) argued that the current technology is more reliable, related services are much cheaper, and the audio and imagery produced is of extremely high quality. In the same work, they further stated that from early systems such as postal services, telegraphs, and printing presses; today's communication technology allows for far greater mass communication and this mass communication is in the form of radio and television, which has been expanded further by cyberspace and associated technologies.

1.1.1 ICT Technologies Usage Precautions

The rapid advancement in wired and wireless communication, as well as the availability of low-cost interoperable devices such as tablets, laptops, and smartphones, has contributed to

the development of several applications such as banking apps and communication apps (WhatsApp) (Jiao, Commuri, Panchal, Milisavljevic-Syed, Allen, Mistree, and Schaefer, 2021; Stewart, Simms, Plale, Link, Hancock, and Fox, 2010). Rana, Singh, and Singh (2021) wrote about the hazards associated with new technical innovations. The advancement of mobile and online applications has empowered handheld devices like mobile phones, tablets, and laptops; however, these devices have also facilitated fraudulent activities involving sensitive personal information (Minnaar, 2019). Mobile technology trends that have enhanced public access include competitive data costs, lower-cost Android smartphones, and lite app technologies designed to function efficiently in low-bandwidth areas (Zamora, 2020). Individualisation of communication technology through personal computers and cellphones has led to an increase in the number of internet users (Mabaso and Kumar, 2018). These advancements and expanding capabilities have increased risks in the use of communication technology and its infrastructure (Storck and Duarte-Figueiredo, 2020). Therefore, security awareness and comprehension of potential threats become critical. This is because users may be subjected to sophisticated sorts of harmful conduct such as identity theft, blackmailing, active data collection, or defamation (Lee and Paek, 2020).

Users must be aware of both the potential risks and the available countermeasures. With the rise in ICT adoption, concerns regarding internet safety have also increased. The significance of ICT, particularly the internet, is surrounded by various threats, attacks, risks, challenges, and vulnerabilities that may lead individuals to security risks (Gilkes, 2022). Cybercrime has been a major concern which has hindered many individuals' acceptance of some ICT services. As a result, assessing how the shift toward new technology will influence the cybersecurity landscape of rural communities before initiating and encouraging cybersecurity awareness is imperative (Patala, 2019).

The cyber world and the internet are dangerous places where innocent users might fall victim to cyberattacks. These risks are exacerbated by the fact that a significant portion of rural communities lack consistent access to technology and broadband internet, leaving rural communities vulnerable to cyber threats. Furthermore, many rural communities cannot deal with these challenges due to the lack of adequate resources (CSIR, 2011).

1.1.2 Cybersecurity

Cybersecurity, which developed in the early 1960s to 1970s, is recognised as a distinct field and continued to expand and be publicly known in the 1980s (Lee, 2021). Due to the cyberattacks and threats faced, cybersecurity has formed part of the modern world. The importance of cybersecurity grows with the increase of internet connection amongst people. In addition to computer use in the 1960s, which involved the use of a single computer by

multiple people, the creation of the first form of the internet called ARPANET realised the need for cybersecurity (Chikalova, Tkachuk, and Lavrinenko, 2021). ARPANET introduced many grounds for new technologies; it enabled the development of new technology such as email (Lessambo, 2023). Malware, which stands for malicious software, was also developed. In this development of malware, the first computer worms known as the Creeper and Reaper were also developed (Asamoah, 2020). In the 1980s, the internet was formed, and what was considered serious chaos in the cyber world occurred during this time, and the real malware was developed during this period, including major events such as a hacker gaining access to sensitive documents from the US military and the creation of a malware called Morris Worm (Chikalova et al., 2021). Initially aimed at only the internet, this worm eventually affected computers and kept on replicating. As the ownership of computers increased in households, the virus spread, making devices connected to the internet vulnerable (Chikalova et al., 2021). In the same work, it is noted that computers used to connect to the internet were particularly at risk. Therefore, the virus attacks then led to the development of anti-malware. This anti-malware industry has since grown to become modern cybersecurity (Akhtar, 2021). The cybersecurity concept has been developing over time and it is now more frequently used than in the past (Lee, Seo, Oh, and Kim, 2021). Cybersecurity has now evolved since cyber criminals have developed innovative ways to conduct and implement cyberattacks (Zevenet, 2022).

Although there are various contested definitions of cybersecurity, Cisco (2020) defined “cybersecurity” as safeguarding businesses' networks and information systems against damage, theft, or unauthorised disclosure of electronic hardware, data, or software. Additionally, it involves preventing the disruption of the services they offer. Large technology and consulting firms like CISCO and McKinsey have developed cybersecurity frameworks with ambiguous foundations tailored to diverse industry applications (Śledziewska and Włoch, 2021). An intensive awareness effort to educate internet and technology users about fundamental security is planned to prevent internet users from falling victim to cyberattacks.

1.2. Problem Statement

Rural communities, particularly in developing countries, are regularly experiencing cyberattacks and typically lack the requisite resources (knowledge and skills) to defend against these attacks (CSIR, 2011). Several studies conducted by various authors such as (Humayun, Niazi, Jhanjhi, Alshayeb, and Mahmood, 2020; Parn and Edwards, 2019) support the idea that rural communities are vulnerable to cyber threats. After all, they lack cybersecurity awareness and inherit the risks posed by the internet because they are frequently underequipped to handle these risks. Mabaso and Kumar (2018) argued that

several cybersecurity awareness campaigns were carried out during the COVID-19 outbreak. However, many of them were conducted to support institutions, businesses, and other organisations with well-structured resources and IT skills.

Rural communities that lack adequate skills to tackle cybercrime need a better strategy to improve their cybersecurity status. Cyberattacks against rural communities have increased because of the rapid advancement in internet-based technology. These attacks are motivated by the lack of a cybersecurity awareness strategy for rural communities, which motivates hackers to frequently target rural communities (Mashiane, Dlamini, and Mahlangu, 2019). Furthermore, in the same work, it is stated that the level of cybersecurity awareness is greater in urban areas than in rural communities because of the easy access to information. Despite the massive efforts and risks to adopt and use the internet, little has been done for rural communities to cultivate a cybersecurity culture (Parn and Edwards, 2019). Therefore, rural communities are at risk since they have few defences against cyberattacks, and the lack of a cybersecurity awareness strategy among rural communities results in a lack of drive to strengthen cybersecurity.

The study aims to fill the gap by developing and implementing a cybersecurity awareness strategy that is specifically designed for rural communities in Limpopo Province. By identifying the cybersecurity challenges unique to these communities and examining the factors influencing cybersecurity policies, this research seeks to contribute to the body of knowledge by offering a framework that not only addresses current vulnerabilities but also fosters a sustainable cybersecurity culture in these rural communities.

1.4. Research Aim

To develop a cybersecurity awareness strategy for rural communities of the Limpopo Province, Mopani District.

1.5. Research Objectives

The study aims to achieve the following objectives:

i. To identify cybersecurity challenges faced by the rural communities of Mopani District.
ii. To investigate the level of cybersecurity awareness in rural communities of the Mopani District.
iii. To determine cybersecurity attitudes in rural communities.
iv. To identify factors that can influence cybersecurity policies in rural communities.
v. To develop a cybersecurity awareness strategy for rural communities of the Limpopo Province, Mopani District.

1.6. Research Questions

The study addresses the following research questions:

i. What are the cybersecurity challenges faced by rural communities of Mopani District in Limpopo Province?
ii. What is the level of cybersecurity awareness among rural communities in the Mopani District of Limpopo Province?
iii. What is the attitude of rural communities towards cybersecurity?
iv. What are the factors that can influence cybersecurity policies in rural communities?
v. What cybersecurity awareness strategy can be suggested or is suitable for rural communities of the Mopani District?

1.7. Justification for the study

There is an exponential increase in users of technology globally as well as in South Africa (CSIR, 2011). Literature indicates that cyberspace continues to change with technological advancement (Brown and Lee, 2019). Cyberspace is evolving into a complex network of interactions, which presents opportunities for cybercriminals (Ngoma, Keevy, and Rama, 2021). For this reason, rural communities regularly experience cyberattacks and have no capabilities to minimise the attacks. The lack of capabilities for tackling cybersecurity attacks is indicative of the internal weaknesses of rural communities. This weakness can be strengthened by research, which was one of this study's goals. The study was therefore justified in four main ways, namely:

- There was a need for sensitisation and advocacy for rural communities in South Africa. A need to demystify the misconceptions that cybersecurity is only for businesses and urban areas with intricate networks.
- Additionally, there was a need to let rural communities acknowledge the exposure they had to the ever-changing cyberspace. The rural communities also needed to be informed on how they can draw benefits from consciously participating and sharing cybersecurity intelligence information. Thus, the need for continual development of new and shared strategies to reduce the level of cybersecurity risks and the frequency of cyberattacks.
- Inclusivity and equal opportunity: By ensuring cybersecurity awareness in rural communities, the study corresponds with the goal of ensuring or creating equal opportunities for all South Africans. It ensures that individuals in rural areas have the same level of protection and awareness against cyber risks as those in urban

areas, thereby promoting inclusivity and reducing the potential for exploitation and harm.

- The study contributed to the existing literature through the development of a cybersecurity awareness strategy for a rural community.
- Additional context for Mopani District: the Mopani District, characterised by its rural setting and limited technological infrastructure, faces unique cybersecurity challenges. Its geographical isolation and limited access to advanced technology exacerbate vulnerabilities and impede effective response to cyber threats. By focusing on this district, the study addresses specific local needs and provides actionable strategies to enhance cybersecurity in similar rural contexts.

- Economic and social impacts: improved cybersecurity in rural areas like the Mopani District can have significant economic and social impacts. Economically, enhanced cybersecurity can prevent financial losses from cyberattacks, support the growth of local businesses, and foster a safer environment for digital transactions. Socially, it can improve the overall quality of life by reducing the risk of cybercrime-related issues such as identity theft and online fraud, thus contributing to the well-being and security of rural residents.

1.8. Delimitations of the study

Delimitations delineate the study's specific boundaries or constraints to refine its scope and emphasis (Creswell and Creswell, 2018). The scope of this study was the rural communities in Limpopo province, Mopani District. Amongst the rural communities of the Mopani District, the study focused on residents of rural villages within Ba-Phalaborwa areas. These villages, including Majeje Benfarm, Humulani, Selwane, Makhushane, and Mashishimale, represent the rural area, providing a clearer definition of the community being studied.

1.9. Operational Definitions

- **Rural Area:** refers to regions located outside urban centres such as towns and cities. These areas are typified by small villages, low population density, and predominantly agricultural activities (Lee, 2021).
- **Cybersecurity:** is the preservation of confidentiality, integrity, and availability of information in cyberspace (Nkurunziza, 2021). In this case, confidentiality means preventing disclosures of clients' data or information to parties not authorised, while integrity means keeping out parties not authorised from data or information so that they do not modify it. Availability is to ensure that authorised persons are allowed to access the data/information as and when required.

- **Cybercrime:** refers to illegal and criminal activity intended to acquire and manipulate data through the use of networks and computer technology for purposes of fraud or theft, abuse, terrorist activities or espionage, or other benefits (Deora and Chudasama, 2021).
- **Vulnerability:** denotes the system weaknesses or cracks that are potential for possible threats that unauthorised parties can exploit (Kure, Islam, and Razzaque, 2018).
- **Cyberattack:** is the exploitation of vulnerabilities within a computer system or in networks by unauthorised persons through the use of malware intending to commit cybercrimes (Goutam, 2021).
- **Cybersecurity Awareness:** is a process of educating and training internet users about cyber threats, how to prevent cyber threats and how to deal with a cyberattack (Richardson, Lemoine, Stephens, and Waller, 2020).

1.10. Research outline

The research is presented in the following manner:

Chapter 1: The background to the study, problem statement, research questions, objectives, and justification for the study were outlined.

Chapter 2: Provided an extensive review of existing literature concerning rural communities and cybersecurity risks. Furthermore, it included available cybersecurity frameworks used in South Africa. Additionally, the chapter entailed the development of the proposed framework for this study, which was linked to the existing literature.

Chapter 3: Outlined the methodology used for data collection and analysis in this study.

Chapter 4: Presented the findings derived from the collected and analysed data.

Chapter 5: Discussed the findings obtained from the data analysis.

Chapter 6: Provided the conclusions drawn from the findings and presented the resulting recommendations.

1.11. Chapter Summary

The chapter presented the background to cybersecurity concerns, vulnerabilities, or risks that may hinder the achievement of rural communities' growth. The vulnerability of rural communities in South Africa concerning cybersecurity-related issues was presented as the research problem. The research justification was presented through highlighting the need to develop a cybersecurity awareness strategy to prevent cyberattacks. Lastly, this chapter presented the research outline.

2. CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

This chapter critically evaluates literature relating to cybersecurity which focused on previous studies and research findings concerning cybersecurity. The chapter achieved a thorough comprehension of the research area by recognising secondary data on cybersecurity as a general term, its challenges, factors, effects, awareness, and its usage in rural communities. According to Breslin and Gatrell, (2023), literature review assists in identifying gaps about a phenomenon for current research and provides context in the study. These gaps identified through the literature review were used to develop the study's research question. A brief overview of cybersecurity in various contexts, as well as its usage in rural communities was explored. Furthermore, this chapter clarified the theoretical frameworks employed and introduced a conceptual framework guiding the study.

Furthermore, the researcher conducted a systematic search across several academic databases, such as Google Scholar, Scopus, and PubMed. The aim of the search was to identify relevant studies addressing cybersecurity awareness in rural communities. Key terms such as 'rural communities', 'cybersecurity awareness', and 'information technology adoption' were used to guide the search process. In addition to academic articles, grey literature such as policy documents and reports were also included to ensure a comprehensive review of the topic. The researcher performed the literature search to identify best practices, current challenges, and trends in cybersecurity awareness strategies for rural populations. Following the initial search, articles were evaluated based on their relevance to the research topic and to the study's inclusion criteria. This process involved reviewing abstracts and full texts to determine their suitability for inclusion in the review.

2.2. An overview of cybersecurity

According to Gonzalez III and Kemp (2019), organised crime groups dominate the criminal market of business cyber-crime globally and affect business digitalization dismally. Cybersecurity is a national security concern. Several countries worldwide have established their national cybersecurity policy and strategies framework (Mabaso and Kumar, 2018), and each of these countries defines cybersecurity differently, as illustrated in Table 2.1. This indicates that there is no universally standardised definition of cybersecurity.

Table 2.1: Cybersecurity by various nations (Mabaso and Kumar, 2018).

	Nations/Countries	Explanation
i.	South Africa	It encompasses risk management policies, safeguards, strategies, assurance, training, tools, best practices, actions, and technologies employed to safeguard organizational assets, cyberspace, and users.
ii.	Uganda	It involves protecting the data and information systems from unauthorised access, use, disruption, modification, destruction, or disclosure.
iii.	Romania	It comprises a set of measures aimed at ensuring the integrity, authenticity, confidentiality, non-repudiation, and availability of information while safeguarding cyberspace and both private and public resources.
iv.	New Zealand	It involves the practice of defending cyberspace and its associated components against attacks, ensuring the confidentiality, availability, and integrity of information, as well and detecting, protecting, and recovering from cyberattacks, among other tasks.
v.	Netherlands	The purpose of cybersecurity is to protect ICT against the risks of destruction, abuse, or disruption.
vi.	India	It involves safeguarding information systems, data, and networks through appropriate technological measures against abuse, destruction, or disruption.
vii.	United Kingdom	Cybersecurity entails safeguarding national interests in the utilization of cyberspace, along with the pursuit of broader national security policy objectives.
viii.	France	Consists of safeguarding cyberspace from events that could compromise the integrity of information systems, as well as the availability, confidentiality, and other services provided by the ICT systems.
ix.	Germany	It involves achieving a requisite state in IT security wherein risks within cyberspace are diminished to an acceptable level.
x.	Canada	It entails mitigating the risks posed by cyberattacks and establishing an appropriate level of response to cyber incidents, unauthorised access, use, disruption, manipulation, or destruction of electronic information and related infrastructure.

		Table 2.1 Continues
xi.	Australia	It is the mechanism for protecting information that upholds the confidentiality, integrity, and availability of stored, processed, and transmitted information through electronic means.

2.3. Cyberinfrastructure

The cyberinfrastructure encompasses data storage systems, computing devices, technological tools, visualization environments, human resources, and data repositories, all interconnected via high-speed networks. This setup facilitates scholarly innovation and discoveries that would otherwise be impractical (Clim, 2019). It can also be described as the infrastructure built upon distributed computers and ICT (Kim and Crowston, 2011). Cyberinfrastructure is also viewed as a technological system that integrates various technologies including processing, storage, communication, hardware, and software (Jiao et al., 2021; Stewart et al., 2010). A hardware is the physical element of a computer (Hodges, Sentance, Finney, and Ball, 2020); software directs the hardware on what it should do and how it should do it such as a computer program (Hodges, et al., 2020); and an application is a computer program that is implemented to perform tasks other than those that relate to the operation of the computer, an example is statistical applications and media players (Adamopoulou and Moussiades, 2020). Humans are a major and important element of cyberinfrastructure. There are two characteristics that distinguish cyberinfrastructure, namely; a) The integration of technological components through software and high-performance networks into a comprehensive system; and b) the resultant enhancement of research productivity and the achievement of breakthroughs once considered unattainable (Srivastava, Venkataramanan, and Hauser, 2023). There are many examples of cyber-infrastructure; amongst them is the future grid which is a project with the aim of being a cyber-infrastructure for computational science (Stewart et al., 2010). In this project, hardware, network and software environment is created and therefore researchers can replicate and perform experimental research. This study encompasses performance analysis within computer and computational science fields. In this endeavor, humans engage with Cyberinfrastructure to develop new software for the future of cyberinfrastructure. Additional, instances of cyberinfrastructure include the Open Science Grid, TeraGrid, Simulation of Gas Giant Planet Formation, Linked Environments for Atmospheric Discovery, and PolarGrid (Stewart, et al., 2010).

There are several advantages associated with employing cyberinfrastructure, particularly in the realm of business. It is widely recognised as an effective approach worldwide for reducing expenses, boosting profits, safeguarding information, and expanding brand influence in the era of Internet operations. This not only enhances understanding of production and sales models but also creates a favorable impression among diverse consumer audiences (Wang, Wei, Qiao, Lin, Chen, 2018). The utilization of cyber-infrastructure aids organizations in promoting and selling both consumable and non-consumable goods, as well as delivering services more swiftly. Online transactions are crucial for enabling product diversity and adapting to changing consumer spending patterns, facilitating more precise, time-efficient purchases, and enabling remote monitoring of actual demand and inflation (Jaravel and O'Connell, 2020). However, this mode of commerce exposes traders, especially, to cyber threats such as data breaches, fraud, and virus attacks, which escalate alongside the increasing adoption of cyber-systems in business (Cavico, and Mujtaba, 2017).

The degree of advancement in cyberinfrastructure directly impacts its security stance (Hasan, Ali, Kurnia, and Thurasamy, 2021). Research suggests that cybercriminals exploit the inadequate security practices prevalent among the general population. Hence, policymakers are urged to conduct awareness campaigns to mitigate the prevalence of cybercrime. There is evidence that 45% to 70% of internet users behavior and cyber-related risks can be reduced by an investment in security awareness and training (Zwilling, Klien, Lesjak, Wiechetek, Cetin, and Basim, 2022).

2.4. The impact of cybercrime

Any illicit activity involving a networked device, computer, or network is classified as cybercrime (Burns and Brush, 2021). Although many cybercrimes are perpetrated with the intention of financial gain, some are targeted at specific systems or devices with the aim of causing harm or disruption. The most common effects of cybercrime are damage to reputation, waste of time, loss of sales, identity theft, loss of revenue, and reduce productivity and among others.

According to Akinwumi, Iwasokun, Alese, and Oluwadare, (2017), data sharing between individuals and businesses is essential for the development and enhancement of technical goods and services. However, occasionally internet users may be ignorant of the many types of cybercrimes, making them vulnerable to cyberattacks. Any organization may experience cybercrimes if a point of entry or vulnerability allows an unauthorised user to access their information (Wadhwa and Arora, 2017). In substantiation, Aishwarya, Pratiksha, Hule, and Sayli (2018) state that one of any market's most valuable assets is information. Since organizations have been storing private data and keeping secret information, data breaches

have been another threat to firm data. According to Marti, Nielsen, Bińkowski, and Donnat, (2021), cyber victimization has serious financial and personal repercussions for the users of internet, and the adverse effects on economy the entire cyberinfrastructure used by businesses and customers seeking services.

According to Moagar-Poladian, Dumitrescu, and Tanase, (2017), the utilization of business cyber-infrastructure has tripled its share of the global GDP, surging from 0.5% to over 1.5% since 2007, marking a noteworthy and rapidly growing industrial trend. Conversely, the overall cost of global cybercrime has experienced a swift escalation, soaring from $445 billion in 2014 to surpassing $600 billion in 2017, indicating a simultaneous increase alongside business cyber-infrastructure on a global scale (McAfee, 2018). Furthermore, while South Africa is adjusting to the new era of digital markets as the rest of the world (Ndung'u and Signé, 2020), especially since after the Covid-19 pandemic (Asamoah, 2020), cyber-crime is a concern, especially in businesses and individuals in rural areas, as cyber-criminals may prey on the less civilised and still-growing systems therein. Cybercrime is rife because the internet was built with an idea to be used in research than the commercial use it has today. For this reason, security was not taken into consideration when designing the internet. Cybercriminals use the ICTs to invade the internet system (Giri and Shakya, 2020).

Cyber criminals are aware that there is a spread of cybersecurity awareness; and they improve their skills of cyberattacks (Tam, Rao and Hall, 2021). Cybersecurity is better in large organizations than in small businesses and personal computers. For this reason, cybercriminals have now turned their attention to small targets (small businesses, personal computers, and smartphones (Geer, Jardine and Leverett, 2020).

In South Africa, internet users had grown to 51% in the year 2018; more of this percentage is owed to smartphones and the internet access they provide (De Doncker and McLean, 2022). Cybersecurity is incorporated in some universities in South Africa. This integration represents one of the initiatives undertaken by the South African government to enhance cyber resilience. Cyber resilience refers to the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, and attacks on systems utilising cyber resources (Zuo, Guo, Gan, and Lu, 2021). However, this cybersecurity education is not catered to everyone in South Africa; rural areas are left vulnerable due to the lack of this kind of education. However, the rural community pupils might have received a glimpse of cyberattacks and cybersecurity in the Life Orientation subject (Venter, Blignaut, Renaud, and Venter, 2019).

2.5. Cybersecurity risks

The significance of cybersecurity is increasing for all stakeholders, encompassing individuals, businesses, and governments, with small businesses particularly affected. Safeguarding data poses one of the most prominent challenges in cybersecurity, especially in a digital landscape where everything, from adorable kitten videos to personal vacation journals and credit card information, is stored online. There are increasing reports of data theft, fraud, system-shutdown, hacking and hate speech. There has been evidence that these reported cyber activities result in fear and anxiety. Therefore, more individuals, institutions and individuals become insecure about using new technology (McGuire, 2022). The increase and usage of networks as a vital business method by small businesses have resulted in exposure to a myriad of cybersecurity challenges. Although the goal is to ensure cybersecurity, there are human errors that also pose a challenge. There are human behaviours that cause a breach in cybercrime and cybersecurity; this is mainly due to not following the rules and regulations put in place when using the internet (Richardson et al., 2020). There are various types of cybersecurity concerns faced by rural communities and businesses, including ransomware, phishing, malware-attack, security threats, denial of service, and more. Since the COVID-19 pandemic, a lot of South African businesses have embraced digitalization to enable operations to continue even during the imposed shutdown. As a result of vulnerabilities in their commercial websites, many companies that have embraced this approach have become susceptible to cyberattacks, including spamming, credit fraud, e-skimming, malware, and phishing attacks (Varghese and Xu, 2022). The most prevalent issues faced by businesses are discussed in sub-sections 2.5.1 to 2.53.

2.5.1. Phishing

A systematic study by Alkhalil, Hewage, Nawaf, and Khan, (2021) has revealed phishing as the most notorious issue faced by businesses and internet users at large; social engineering crime gives way to the attacker in performing identity theft. In the same study, the researchers further argue that phishing entails a fraudulent activity wherein a replica of an existing web page is created to deceive a user into divulging personal, financial, or password information. More precisely, Lee and Paek, (2020) define phishing as a type of social engineering, wherein an attacker, also referred to as a phisher, endeavors to deceitfully obtain confidential or sensitive credentials from legitimate users by imitating electronic communications from a reputable or public organization in an automated manner. Such communications are commonly executed through emails that direct users to deceptive websites, which then gather the targeted credentials.

In the United Kingdom, businesses have witnessed a surge in phishing attempts, escalating from 72% to 86% between 2020, with a significant portion of these attacks originating from social media platforms (GOV.UK, 2020). The evolution, propagation, and dissemination of reported phishing assaults are monitored by the Anti-Phishing Working Group (APWG). The APWG functions as an international coalition comprising responders to cybercrime, forensic investigators, law enforcement agencies, technology firms, financial institutions, academics, non-governmental organizations (NGOs), and non-profit organizations (NPOs) (Halouzka et al., 2021). The APWG has a focus on the elimination of identity theft, and frauds. These are issues brought upon by the increase of phishing, crimeware and hacking of emails (Correia, 2021). The APWG services are rendered to financial institutions, online retailers, law enforcement and government agencies (Sonowal and Sonowal, 2022). Their mission is to consolidate the global response to cybercrime by facilitating data exchange, conducting research, and raising public awareness.

The reports received by the APWG are analysed and quantified in the APWG Phishing Activity Trends Report, published on March 21, 2021. In the United Kingdom, the number of phishing attacks surged to 266,387 in the third quarter of 2019, marking the highest figure in three years since late 2016. This nearly doubled the 138,328 attacks recorded in the fourth quarter of 2018 and represented a 6% increase from the 182,465 attacks in the second quarter. The same report also indicated that during the same quarter, 118,260 distinct phishing emails were reported to the APWG, targeting 1,283 different brands (GOV.UK, 2020).

2.5.2. Malware, spyware, and ransom-ware attack

In digital environments, computer users encounter various threats including worms, spyware, phishing, viruses, malware, and ransomware, among others. Malware, characterised by its malicious intent, operates counter to the interests of computer users and thus excludes software that causes unintentional harm due to deficiencies (Minnaar, 2019). Even officially provided software by businesses may be classified as malware if it covertly acts against the user's best interests. One notable example is the Sony rootkit, a Trojan horse embedded within CDs distributed by Sony to prevent unauthorised copying. It not only monitored users' listening habits but also inadvertently introduced vulnerabilities exploited by other malware to compromise victims' computers (Minnaar, 2019).

A study conducted by Talukder and Talukder, (2020) revealed that authors of spyware employ spyware to assault users with malevolent intentions. Various computer viruses and worms, such as Melissa Macro Virus, Explore, Zip worm, Nimda, Code Red, Slammer, and Blaster, are known to inflict damage on files and hard drives. These attacks, often likened to system terrorists, seek to undermine credibility, compromise national security, inflict widespread harm,

deplete resources, exploit critical systems, weaken the economy, undermine public morale, and erode public confidence. Terrorists may employ spyware to examine the targeted systems to make income or acquire crucial information for a subsequent strike (Smith, Smith, Burger, and Boyle, 2023). According to Sen, Jena, Jena, and Devabalan, (2022), spyware normally uses identity theft, which involves overtaking individual user accounts of people and organizations; stalking, which involves using social media interface that shares photos, whereabouts, contact information, interests, as well as communication rights with friends and acquaintances; sexual predation, which involves illegally uploading or sending sexual content to an unsuspecting internet user.

Ransomware operates as an extortion scheme where perpetrators seize and encrypt the victim's computer files, subsequently demanding a ransom for their release in their original state (Humayun et al., 2020). According to Kaspersky, a leading global antivirus company, ransomware poses a significant threat due to the lack of means to recover the compromised data (Filiz, Arief, Cetin, and Hernandez-Castro, 2021). This malicious software exploits vulnerabilities in a user's computer to infiltrate and encrypt all files, withholding them until the victim pays the demanded ransom (Minnaar, 2019). Typically, in a ransomware attack, the perpetrator gains access to a compromised computer by exploiting exposed system vulnerabilities (Humayun, et al., 2020).

2.5.3. Credit card fraud

According to Makki, Assaghir, Taher, Haque, Hacid, and Zeineddine, (2019), credit card fraud encompasses various types. Additionally, the same study proposes distinguishing credit card fraud based on the tactics employed by fraudsters, which include behavioral and application fraud. Minnaar, (2019) outlined six categories within the credit card fraudulent transactions process, including frauds involving lost or stolen cards, frauds involving counterfeit cards, online frauds, frauds involving bankruptcy, merchant frauds, and frauds involving cards stolen during the expedition process. Jain, Tiwari, Dubey and Jain, (2019) suggest that credit card fraud can be categorised into in-person (card-present) fraud and online (card-not-present) fraud. Furthermore, Varmedja, Karanovic, Sladojevic, Arsenovic, and Anderla, (2019) noted that financial fraud strategies have evolved from traditional methods, such as data audits to identify fraudulent transactions, to computational approaches leveraging statistics and artificial intelligence.

2.6. Cybersecurity risk management frameworks

For security leaders in various countries and businesses, a cybersecurity framework provides a standardised language and set of norms that enable them to comprehend their security postures as well as those of their providers (Akinwumi, Iwasokun, Alese, and Oluwadare,

2017). Cybersecurity frameworks consist of documents delineating guidelines, standards, and best practices tailored for cybersecurity risk management (Culot, Fattori, Podrecca, and Sartor, 2019). Their study further states that these frameworks are designed to mitigate an organization's exposure to weaknesses and vulnerabilities that could be exploited by hackers and other cybercriminals. Implementing a framework facilitates the specification of steps an organization must take to assess, manage, and mitigate cybersecurity risks (Lee, 2021). Common cybersecurity frameworks include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Control Objectives for Information and Related Technologies (COBIT) Enterprise Risk Management Framework, the International Organization for Standardization/ the International Electrotechnical Commission (ISO/IEC) 27001:2013, the Information Technology Infrastructure Library (ITIL) Framework, and Control Objectives for Information and Related Technologies (COBIT).

2.6.1. NIST Cybersecurity Framework

The NIST Cybersecurity Framework serves as a voluntary framework assisting organizations of all sizes in comprehending, managing, and mitigating their cybersecurity risks, thereby safeguarding their networks and data (Taherdoost, 2022). According to Shukla, Katt, Nweke, Yeng, and Weldehawaryat, (2022), the fundamental premise of this framework is to ascertain whether the organization has a formal security program in place and comprehends its security posture. Moreover, the framework aims to identify what is protected, assess the adaptability and repeatability of security practices, and ascertain whether they align with the organization's business and mission requirements. Additionally, the framework identifies gaps and devises a roadmap for improvement. While this framework may appear as "common sense," its simplicity is considered its strength as it establishes a common framework for managing cyber risk (Hamdani, Abbas, Janjua, Shahid, Amjad, Malik, Murtaza, Atiquzzaman, and Khan, 2021).

According to NIST (2018), the NIST Cybersecurity Framework was developed to minimise cyber risk and enhance the security of critical infrastructure. It draws upon standards such as COBIT, ISO, and IEC. The framework aims to provide organizations with a standardised approach to:

- **Assess the current cybersecurity state or posture:** This involves evaluating the existing cybersecurity measures, policies, and practices within the organization to understand its strengths, weaknesses, and areas for improvement. This assessment may involve conducting security audits, risk assessments, and vulnerability scans to identify any vulnerabilities or gaps in the organization's cybersecurity defenses.

- **Define the intended cybersecurity state:** Based on the assessment of the current cybersecurity posture, organizations can define their desired cybersecurity state. This includes establishing specific goals, objectives, and targets for improving cybersecurity posture, such as implementing new security controls, enhancing employee training and awareness, or strengthening incident response capabilities.

- **Identify and prioritise improvement opportunities:** Once the current and intended cybersecurity states are defined, organizations can identify and prioritise opportunities for improvement. This involves identifying specific areas where cybersecurity measures can be enhanced or gaps can be addressed to move closer to the desired cybersecurity state. Improvement opportunities may include investing in new security technologies, enhancing employee training programs, or improving incident response processes.

- **Evaluate progress towards the desired cybersecurity state:** Organizations should regularly evaluate and assess their progress towards achieving the desired cybersecurity state. This involves monitoring key performance indicators (KPIs), metrics, and milestones to track progress and identify any deviations from the planned trajectory. Regular progress evaluations enable organizations to make informed decisions, adjust strategies as needed, and ensure continuous improvement in cybersecurity posture over time.

- Engage stakeholders internally and externally to raise awareness about cybersecurity risks. As noted by Gordon, Loeb, and Zhou, (2020), it is essential to understand that cybersecurity frameworks are not one-size-fits-all solutions, as different organizations encounter diverse cybersecurity threats. These frameworks are tailored for businesses, non-governmental organizations, government agencies, and various communities.

  The framework consists of three main components: the framework core, implementation tiers, and framework profile. As detailed by NIST (2018), the NIST Framework encompasses five sub-components or activities: identify, protect, detect, respond, and recover, as depicted in Figure 2.1.

Figure 2.1: NIST Cybersecurity Framework (Source: NIST, 2018).

The NIST framework can be viewed as a comprehensive collection of cybersecurity activities, goals, and references applicable across industries. It comprises a total of 98 subcategories and 22 categories for each function (Angelini, Lenti, and Santucci, 2017). In the same study, it is stated that subcategories represent practical tasks that organizations must undertake, such as gathering data on software and hardware or documenting legal cybersecurity requirements. International standards associated with each category and subcategory serve as informative guidelines. Implementation of all subcategories can elevate an organization's cybersecurity posture significantly.

It is important to recognise that while the cybersecurity framework was initially developed for critical infrastructure, it can also benefit smaller businesses and communities (Kwon, Ashley, Castleberry, Mckenzie, and Gourisetti, 2020). Critical infrastructure includes assets and systems vital to a country, the disruption of which could severely impact economic well-being, public health, safety, and national security. Examples of critical infrastructure include power grids, healthcare systems, and transportation networks. Although the framework was primarily intended to safeguard the highly developed infrastructure of the United States, it can be adapted for use in other countries, including South Africa.

However, it is crucial to acknowledge that a framework tailored to the cybersecurity needs of small businesses would be more practical and supportive of their unique challenges. This recognition prompted the need for developing a cybersecurity strategy specifically tailored to rural communities in the Mopani District. For these communities, the NIST Cybersecurity Framework may be deemed unnecessary, as some subcategories are only relevant for critical infrastructure.

2.6.2. COSO Enterprise Risk Management Framework (COSO-ERM)

According to Yuan, (2022), the COSO-ERM framework stands out as one of the most comprehensive frameworks designed to provide organizations with a widely accepted framework for evaluating their risk management initiatives. It adopts a principles-based approach, leveraging internal control concepts to offer a more robust focus on Enterprise Risk Management (ERM). Recognising the importance of integrating ERM processes into the development of cybersecurity strategies, this framework provides recommendations to help businesses establish effective systems for identifying, quantifying, prioritising, and managing risks (Dan Perbankan, 2021).

Comprising eight interconnected components, the COSO-ERM framework includes:

a). Internal Environment: This component emphasises the organization's tone, risk appetite, and elements such as board oversight.

b). Objective Setting: Focuses on establishing strategic plans and foundational elements for operations, reporting, and compliance objectives.

c). Event Identification: Involves identifying potential events that could impact the business.

d). Risk Assessment: Considers the extent to which potential events may affect the organization's objectives.

e). Risk Response: After assessing known risks, management determines response plans, including avoidance, reduction, sharing, and acceptance.

f). Control Activities: Addresses the policies and processes for implementing risk responses by management.

g). Information and Communication: Ensures that relevant information is identified, captured, and communicated in a timely and appropriate manner to the relevant individuals.

h). Monitoring: Involves evaluating risk management activities and components over time and making necessary adjustments (Yuan, 2022; Anders, 2019).

2.6.3. ISO/IEC 27001:2013

ISO 27001:2013 is a standard for information security management systems aimed at providing a comprehensive framework for companies to implement security principles and practices within their operations. The security management system forms a crucial component of a broader management framework grounded in a business risk strategy, enabling

organizations to manage, implement, operate, monitor, maintain, and improve information security (Lee, 2021).

As highlighted by Al Faruq, Herlianto, Simbolon, Utama, and Wibowo, (2020), this framework encompasses eleven aspects commonly known as control objectives, which are essential for every company aiming to implement effective information security measures. These control objectives serve as guidelines for implementing information security concepts and practices. In this context, controls refer to various elements such as processes, procedures, policies, and tools utilised to prevent undesirable events, such as unauthorised access to data or confidential company information, in alignment with the principles of information security.

2.6.4. The ITIL Framework

The objective of information technology management is to explore and grasp information technology as a corporate asset that influences the strategic and operational capabilities of a firm in developing products and services aimed at maximising customer satisfaction, corporate productivity, profitability, and competitiveness (Nkurunziza, 2021).

ITIL, with its comprehensive checklist, tasks, and procedures, offers a precise definition of several essential practices that can be tailored to suit any organization. ITIL is widely recognised as the most commonly adopted approach to IT service management globally (Gunawan, 2019). This framework has two main objectives, firstly, service **delivery** which is primarily focused on the proactive and forward-thinking services that an organization needs from its ICT supplier to support its users effectively. Secondly, the **service support**, which has a goal that is centered on the ICT service user, which is to make sure they have access to the right services to support the business processes (Al-Ashmoery, Haider, Haider, Nasser, and Al-Sarem, 2021).

2.6.5. The COBIT Framework

COBIT is a highly regarded open standard that is gaining popularity among a diverse range of organizations worldwide (Carlos, 2021). It is recognised as the premier control framework for aiding organizations in aligning the use of information technology (IT) with the business goals of the organization. This is because the COBIT framework has control objectives that focus on the business needs (Abdulrasool and Turnbull, 2020). ISACA (2011) indicates COBIT as one of several solutions through its services. These services include the implementation, service management and assurance guides, low-level practices, and mapping to related frameworks and standards.

In a study by Steuperaert (2019), the COBIT framework is structured around five guiding principles, including: (a) satisfying stakeholder needs; (b) fully encapsulating the company; (c) employing a single, integrated framework; (d) supporting a comprehensive approach; and (e) distinguishing governance from management. Each of these principles draws upon concepts and insights from general management, accounting, and IT literature. Table 2.2 provides a list of existing frameworks.

Table 2.2: Summary for Cybersecurity Frameworks (Adapted from Nkurunziza, 2021).

Framework Name	Organization(s)	Description(s)	Source
NIST	NIST	• This framework offers a comprehensive risk management structure. • Its controls are adaptable and can be readily tailored and integrated into an organization's broader risk management strategy.	(NIST, 2018)
		Its categories include: - Identify: Creating an organizational comprehension to oversee cybersecurity risk across systems, personnel, assets, data, and capabilities. - Protect: Establishing and executing suitable measures to guarantee the provision of vital services. - Detection: Formulating and executing suitable measures to recognise cybersecurity incidents. - Response: Formulating and executing suitable measures to address identified cybersecurity incidents. - Restoration: Formulating and executing suitable measures to uphold resilience plans and reinstate any affected capabilities or services post-cybersecurity incident.	(Teoh et al., 2017)
COSO	COSO	• Offers a structured method for designing and evaluating internal controls. • Highlights management's role in decision-making processes regarding policies and procedures.	(Dangi et al., 2020)

ISO 27001:2013	ISO	• Offers a standardised approach to information security management. • One limitation of the ISO standard is its focus on desired outcomes without specifying the necessary actions to achieve them.	(Garcia et al., 2020)
Table 2.2 Continues			
COBIT	ISACA	• COBIT delineates inputs, outputs, objectives, key activities, and performance measures for each process. • Implementing COBIT can be challenging due to the framework's lack of technical support and detailed guidance.	(Garcia et al., 2020)
ITIL	ITIL	• It aligns ICT resources with business objectives and enhances visibility into internal processes. • Implementation requires significant dedicated resources and is a demanding endeavour. • Embracing ITIL often necessitates cultural changes within organizations to adopt new processes.	

2.6.6. Synthesis and application of cybersecurity risk management frameworks in rural contexts.

Each cybersecurity framework presents distinct strengths and limitations. The adaptability of the NIST framework allows for flexible implementation, however, its comprehensive scope may present challenges for smaller organizations with limited resources. The COSO-ERM framework's emphasis on internal controls is advantageous for managing diverse risks in rural businesses; however, the resource-intensive nature of its implementation could pose significant barriers. While ISO/IEC 27001:2013 offers a universally applicable structure for

systematic security management, its full adoption may prove impractical in environments constrained by limited resources. The ITIL framework, with its focus on optimising IT processes, holds potential for improving service management in rural settings, although the requisite IT expertise may not always be available. COBIT, with its strong governance framework, ensures alignment between IT and business objectives, making it particularly beneficial for smaller enterprises that require efficient resource integration.

Given these considerations, a tailored approach that selectively incorporates elements from each framework aligned with the specific needs and capacities of rural businesses could yield the most effective cybersecurity risk management strategy. For example, the flexibility of the NIST framework could be leveraged for overarching cybersecurity practices, while COSO-ERM's structured risk assessment could provide a robust foundation. Integrating the essential principles of ISO/IEC 27001:2013 for baseline security, alongside ITIL's alignment of IT services with business needs and COBIT's governance mechanisms, can culminate in a hybrid framework that is both practical and effective for rural enterprises.

2.7. Factors that influence cybersecurity policy.

Cybersecurity policy is shaped by a variety of factors, each exerting distinct pressures that can significantly impact the effectiveness of policy implementation, particularly in rural settings. According to CyberVentures (2019), key factors include technological advancements, regulatory environments, economic conditions, and the evolving threat landscape. Chang and Coppel (2020) highlight organizational culture, resource availability, and leadership commitment as additional influences, while Young, van Vliet, van de Ven, Jol, and Broekman (2018) emphasise the role of education, awareness, and stakeholder engagement.

In rural contexts, these factors often interact in complex ways, amplifying the unique challenges these communities face. For instance, the economic constraints commonly experienced in rural areas can exacerbate the difficulty of adopting advanced technologies or complying with stringent regulatory requirements, as identified by CyberVentures (2019). Limited resources, both financial and technical, hinder the ability of rural organizations to implement comprehensive cybersecurity measures, making them more vulnerable to cyber threats. The lack of local expertise and IT infrastructure, highlighted by Chang and Coppel (2020), further complicates policy implementation, as rural communities may struggle to develop and maintain the necessary cybersecurity frameworks.

The cultural aspects noted by Chang and Coppel (2020) also play a crucial role in rural settings. In communities where there is limited awareness or understanding of cybersecurity risks, the adoption of cybersecurity policies may be met with resistance or complacency. This underscores the importance of education and awareness, as stressed by Young et al. (2018), in driving stakeholder engagement and fostering a culture of cybersecurity within rural organizations. Moreover, the relative importance of these factors can vary significantly in rural contexts. For example, while technological advancement is a key driver of cybersecurity policy in urban areas, in rural settings, the immediate concern might be the basic availability of secure IT infrastructure. Similarly, leadership commitment, which is critical according to Chang and Coppel (2020), may be less influential in rural areas where leadership roles are often diffuse and less formalised.

While the reasons for cyberattacks vary, most of them are recurrent and the top three ways that organizations allow criminals to include *Lack of security assistance, System vulnerabilities,* and *Assessing risks* (CyberVentures, 2019). Chang and Coppel (2020) identify three core cybersecurity concerns in developing countries; poor security hygiene, atypical usage patterns, and difficulties in distributing security instructional materials. These challenges are significant due to the unique technological landscape in developing regions,

where reliance on mobile technology is high, and awareness of cybersecurity threats is relatively low.

In contrast, Venter et al. (2019) examined cybersecurity awareness in South African rural communities, particularly focusing on smartphone usage. Their findings align with those of Chang and Coppel (2020), especially concerning the atypical usage patterns and low awareness of cybersecurity threats. Venter et al. (2019) also emphasise the challenges posed by low digital literacy, which exacerbates the difficulties in disseminating security-related information, a point also highlighted by Chang and Coppel (2020).

Comparing these findings with Bada, Solms, and Agrafiotis (2019), who explored cybercrime in African rural areas, reveals further consistencies. Bada et al. (2019) found that the combination of poor security practices and limited access to cybersecurity resources makes rural communities particularly vulnerable to cyber threats. This mirrors the issues identified by Chang and Coppel (2020) regarding the distribution of security instructional materials and the prevalent use of pirated software, which may increase exposure to cyber risks.

However, some differences are evident when comparing these studies with those conducted in other developing regions. For instance, in Southeast Asia, Nguyen and Chib (2019) found that while there are similar challenges in cybersecurity awareness, there is a higher emphasis on community-based solutions and localised cybersecurity practices. This contrasts with the findings of Chang and Coppel (2020) and Venter et al. (2019), who highlight the need for top-down policy interventions and educational programs to improve cybersecurity hygiene and awareness.

A systematic review study conducted by Young, Van Vliet, Van de Ven, Jol, Broekman, (2018) argued that it is not in every case where intruders just attack a system, but humans operating within a firm can contribute to a firm falling victim to cybercrime. Corallo, Lazoi, Lezzi, and Luperto, (2022) termed these individuals as "insiders," denoting employees or other individuals with access, privileges, and deep understanding of internal organizational processes, potentially enabling them to exploit vulnerabilities (Li, He, Xu, Ash, Anwar, and Yuan, 2019).

According to Habibzadeh et al. (2019), these internal humans are classified into three categories, namely a) Employee security policy breaches could be unintentional, like when they unintentionally download dangerous software; b) Employees may engage in voluntary actions that are not motivated by ulterior motives. As an illustration, using cloud computing tools (like Dropbox) even though one is unaware that this is against company policy (also known as "Shadow IT"); and c) insiders who knowingly break rules for nefarious reasons, such

as leaking confidential information to the public. Young et al. (2018) state other common mistakes include utilising unidentified USB sticks, charging a smartphone on a laptop that is used for business, and creating opportunities for eavesdropping and shoulder surfing.

Mabaso and Kumar (2018) discusses types of system issues that attract cybersecurity risk and policy as follows:

- **Accidental Disclosure:** Involves mistakenly sharing sensitive information on a public website or sending it to the wrong recipient via email or other channels.
- **Phishing/Social Engineering:** Occurs when an outsider gains unauthorised access through social engineering tactics, such as phishing emails, malware attacks, or unauthorised USB drives, to acquire an insider's credentials.
- **Physical Records:** Relates to lost, discarded, or stolen non-electronic records, such as hard-copy documents.
- **Portable Equipment:** Involves lost, discarded, or stolen data storage devices, such as laptops, smartphones, USB drives, CDs, hard drives, or data tapes, which could be accessed by an outsider. The human element is crucial in attacks targeting specific individuals or organizations.

Overall, the same study asserts that in most cases hackers apply social engineering activities to obtain access to an organizational network.

2.8 Cybersecurity Awareness

Cybersecurity involves a combination of technologies, processes, controls, and user behaviors aimed at safeguarding systems and their data (Nagyfejeo and Von Solms, 2020). With global cybercrime rates on the rise, Africa has seen an unprecedented increase, which has hindered strategic, social, and economic development. This surge in cybercrime is largely attributed to a lack of cybersecurity awareness (Bada, Solms, and Agrafiotis, 2019). Combatting cybercrime in Africa requires a comprehensive cybersecurity awareness strategy that aligns with the unique challenges faced by different communities, including rural areas.

In rural South Africa, the implementation of cybersecurity awareness presents distinct challenges. Limited access to technology, infrastructure, and education often exacerbates the vulnerability of these communities to cyber threats. Unlike urban areas, where there may be more resources and infrastructure to support cybersecurity initiatives, rural areas require strategies that are contextually relevant and feasible given their constraints. For instance, cybersecurity awareness programs in rural areas must consider the lower levels of digital

literacy and the scarcity of IT professionals. Thus, the content and delivery of such programs need to be tailored to ensure they resonate with and are accessible to rural populations.

2.8.1 Factors that influence the implementation of cybersecurity awareness.

Chang and Coppel (2020) discuss the role of psychological theories in shaping effective cybersecurity awareness programs, noting that behavior change requires more than just information dissemination; it necessitates a deep understanding of the audience's cultural and environmental context. In rural South Africa, cultural norms and local practices significantly influence how cybersecurity messages are received and acted upon. For example, cybersecurity campaigns that align with local values and are delivered in the native languages are likely to be more effective than those that do not. The perception of risk, as influenced by cultural and environmental factors, is another critical consideration. In rural areas, where the immediate threats posed by cybercrime may not be as apparent as in urban centers, cybersecurity awareness programs must work harder to make the risks tangible and relevant. This could involve using analogies or scenarios that reflect the everyday experiences of rural residents, thereby making the concept of cybersecurity more relatable and urgent.

To impact change, people should understand and apply advice given; there has to be motivation to apply the change; and they need to change their attitude and intentions (Bada et al., 2019). These psychological theories were clearly laid out in their study, they describe the psychological theories that influence online behavior as follows:

a) The Regulatory Focus theory: this theory is driven by personal factors such as personal motivation and personal ability influence the change in behavior.

b) The perception of risk theory is guided by cultural and environmental factors. In this regard, when a campaign is conducted, there are cultural characteristics of the audience (people) that need to be known. The message being sent out is more positively received when they match the cultural norms of a recipient.

Chang and Coppel (2020) further revealed factors that can be adopted to enhance the effectiveness of cybersecurity awareness namely:

- There must be professionalism when preparing and organising security awareness.
- There must be avoidance of using fear as it has been proven to be an ineffective tactic when trying to spread cybersecurity awareness. Cybercrimes should not be exaggerated because this creates reluctance to use the internet and the awareness message is therefore misdirected.

- Cybersecurity education must be actionable and practical rather than being information given to internet users. Explanation of how cybercrimes are done and who cybercriminals are helps in making cybersecurity awareness clearer.
- Internet users need to be kept engaged by providing feedback on strategies of cybersecurity; that way it is easier to see the cybersecurity strategy. Cybersecurity should not only be given a security benefit. Other benefits such as the economic benefit for instance should be included.
- When dealing with rural communities, the cybersecurity awareness strategies put in place should be in a rural context. That way the strategy is relatable and doable; personalization leads to better recognition.

2.8.2 The cybersecurity education in the South African context

Most of the South African population owns smartphones; irrespective of whether they are rural or urban based. Therefore, it is imperative that internet users are aware of what they need to do in order to secure their devices (Venter, et al., 2019). Every internet user needs to know that they are vulnerable to attack and will have to find ways to ensure security. A method in which internet users can be aware of cybersecurity is through education. There are two elements in cybersecurity education: a) internet users must be aware that they need to take precautions when using the internet; and b) skills that ensure the effectiveness of cybersecurity precautions have to be imparted. Education on cybersecurity emphasises that cyber awareness is a prerequisite of effective cybersecurity (Mashiane, Dlamini and Mahlangu, 2019).

2.8.3 Cybersecurity Awareness campaigns in South Africa

In South Africa, a significant portion of the population owns smartphones, including those in rural areas (Venter et al., 2019). However, awareness and education on how to secure these devices remain limited, particularly in rural regions where educational resources are scarce. Effective cybersecurity education in these areas must address the dual challenges of raising awareness about the need for security and imparting the necessary skills to implement it.

Traditional methods of cybersecurity education, such as posters, competitions, and adverts, may not be as effective in reaching rural audiences due to logistical and cultural barriers. Instead, more innovative approaches that leverage existing community structures, such as schools, religious organizations, and local leaders, can be more successful. These approaches should focus on the practical application of cybersecurity principles in everyday life, ensuring that the information is not only understood but also actionable.

Any individual, institution or organization that uses the internet cannot ignore cyberattacks. In order not to fall victim to cyberattacks is to have skills and knowledge about cybersecurity. However, skills and the knowledge of cybersecurity is foreign to most internet users. The lack of cybersecurity awareness therefore creates an opportune environment for cyber criminals. A study by Mashiane et al. (2019) states that South Africa has faced various cyber threats, including the ViewFines license scam, email hacks, the Ster-Kinekor attack, the Facebook personal information scandal, and the Master Deed's data leak. These incidents have underscored the importance of cybersecurity for numerous organizations in South Africa (Niselow, 2018). However, when organizations improve their cybersecurity systems, they should also equip their employees. There are factors that can hinder cybersecurity awareness amongst individuals, organizations, and institutions. These factors are the lack of *funding*, the lack of *experts* regarding cybersecurity, the *division in understanding* amongst individuals and the *location* in which individuals, organization or institution is based (Niselow, 2018). There have been strategies such as the use of posters, competitions, books, and adverts to provide cybersecurity awareness. However, these strategies are not effective when dealing with a larger group. Therefore, strategies that are effective in reaching many audiences are needed.

2.8.4 Basics of Cybersecurity Awareness Goals and awareness campaign

According to Corallo et al. (2022), cybersecurity awareness campaign is comprised of goals, plans, expected results, objectives, risks, and methods. There are elements highlighted by Mashiane et al. (2019) that need to be incorporated for a good cybersecurity campaign and these involve:

a) **Cybersecurity Awareness Goals and Objectives:** this must be defined in terms of the national legislation, laws, policies, and standards as well as continental policies and agreements.

b) **Identify Intended Audience:** these are the target trainees, to whom the cybersecurity awareness campaign will be delivered for example, community citizens, IT employees, non-IT employees, students, and learners.

c) **Define Topics to be Covered:** the list of topics must be evaluated in terms of relevance to each targeted audience.

d) **Define Delivery Methods to be Used:** this includes the way in which the cybersecurity awareness campaign will be presented to different audiences for

example, for the primary learner, one can use cybersecurity posters and drawings; and for the employees, one can use e-mail system, company newsletter, and seminars.

e) **Develop a Strategy for Rollout:** this should be decided on all levels and the entire programme should be evaluated for possible loopholes.

f) **Develop Evaluation Methods:** these are the methods that will be used to test the effectiveness of the cybersecurity awareness campaign, for example, the comparison of pre- and post-survey. The cybersecurity awareness plan can be updated to suit various target audiences.

2.8.5. Tailoring cybersecurity awareness campaigns for rural communities.

The effectiveness of cybersecurity awareness campaigns in rural South Africa depends on their ability to meet the specific needs of these communities. Campaigns must be designed with clear goals, objectives, and delivery methods that consider the local context. For example, using visual aids or storytelling techniques that reflect local customs can enhance engagement and understanding among rural audiences.

Moreover, the delivery methods must be adapted to the realities of rural life. In areas with limited internet access, traditional online campaigns may need to be supplemented with face-to-face interactions, community workshops, or mobile-based education initiatives. The involvement of local leaders and influencers can also help in disseminating information more effectively, as these individuals often command respect and trust within their communities.

2.9. Theoretical Framework

The theoretical framework serves as the structure that can underpin or support the theory of a research study (Nord, Koohang, and Paliszkiewicz, 2019). Theoretical framework guides research, which specifies the variables the researcher will measure and the statistical associations the researcher is looking for. It provides theories that describe why the problem being studied exists. As a result, the theoretical framework is a framework that serves as a foundation for conducting research (Varpio, Paradis, Uijtdehaage, and Young, 2020).

Several studies have been undertaken in the study field of cybersecurity. The literature was compiled from a selection of these studies to fulfill the research objectives of this study. According to Rubio, Valero, and Llopis-Albert (2019), a theoretical framework is the review of the main theories that impact current research.

For this study, the researcher adopted the following theories:

- General Deterrence Theory.
- Game Theory.
- Activity Theory.

2.9.1. General Deterrence Theory

Various countermeasures, such as training and awareness campaigns, backups, and disaster recovery procedures, can be employed to mitigate hazards, risks, and threats. Deterrence measures, including awareness-raising initiatives for cyberspace users, support programs aimed at combating criminal violations of cyberspace (Siponen, Soliman, and Vance, 2022). Their study further states that the main components of the General Deterrence Theory are deterrence, prevention, detection, and remedy. The risk management approach to cybersecurity realigned by the General Deterrence Theory makes it a pivotal pillar for this study, which aim to develop a cybersecurity awareness strategy for enhancing the protection of rural communities and users against cyberattacks. Figure 2.2 provides a graphical representation of the theory.

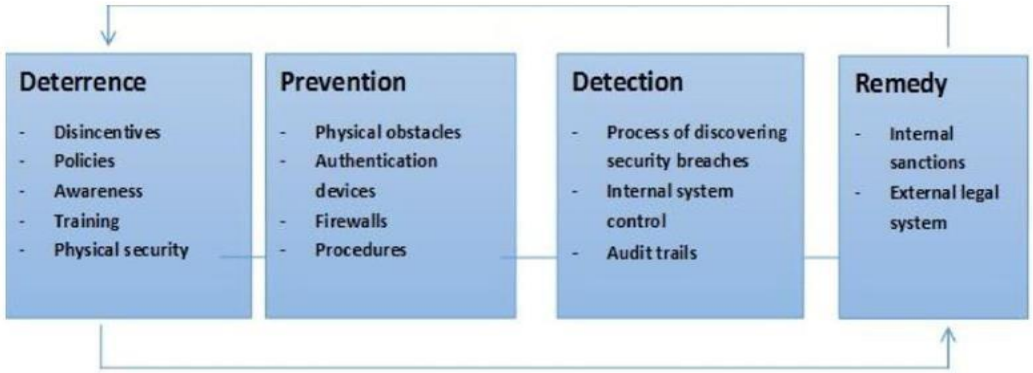

Figure 2.2: Core Elements of the General Deterrence Theory (GDT) (Source: Schuessler, 2009).

2.9.2. Game Theory

In Game theory, every game involves two or more players who make decisions based on strategies that maximise the rewards they anticipate from participating in the game (Chukwudi, Udoka, and Charles, 2017). In the same study, it is stated that each player selects actions that they believe will yield the best rewards for themselves, while also considering the expected actions of other players (opponents). A player could represent a machine, an individual, or a group of people in a game and is responsible for decision-making and subsequent actions (Chukwudi, et al., 2017). Game theory explores the conflict between cyberattackers and cyber victims in the realm of cybersecurity, where their decision-making processes intersect. The

theory's ability to analyse potential cyber threat scenarios within a cyber-system is its core component (Maschler, Zamir, and Solan, 2020). In this study, Game theory will provide valuable guidance for resource allocation and policy implementation, considering the dynamic nature of cybersecurity threats and cyberspace. Additionally, it will emphasise that the primary players in the game are cyber attackers and grassroots cyberspace users, underscoring the importance for rural communities to anticipate and counteract cyberattacks effectively.

2.9.3. Activity Theory

According to the Activity theory, optimal aging happens when people engage in activities, interests, and relationships. The Activity theory was developed by the Russian researcher, which was translated into English in 1978 (Choi, Cho, and Lee, 2019). The study further states that the theory centers on how humans interact with their environment, influenced by factors such as history, culture, and individual psychology, and it was extended through breaking down an activity into component which is the objects, tools, subjects, rules, tasks, and tools through the division of labor to accomplish a goal and are controlled by rules or laws established by the society that specify the parameters of the activities that must be carried out.

Pham, Brennan, and Furnell, (2019), applied this theory to cybersecurity, investigating how the experience of non-technical employees, as well as social and cultural factors, influence the occurrence of cybersecurity breaches resulting from disregard for norms or non-compliance with policies and procedures. Utilising this theory in the study will facilitate understanding the relationship between cybersecurity readiness in rural communities and the behavior of residents, aiming to ensure cybersecurity preparedness.

2.9.4. Synthesis of theoretical insights.

The interplay between General Deterrence Theory, Game Theory, and Activity Theory provides a robust foundation for understanding and enhancing cybersecurity awareness in rural communities. General deterrence theory emphasises the importance of deterrence measures, such as awareness campaigns, to prevent cybercrimes by increasing the perceived risks for potential offenders. This theory highlights the critical role of preventative actions in reducing the likelihood of cyberattacks in resource-constrained rural settings. Game Theory complements this by analysing the strategic interactions between cyber attackers and defenders, underscoring the need for rural communities to anticipate and respond to cyber threats dynamically. It illustrates how rural users can employ strategic thinking to mitigate risks and optimise their limited resources for maximum protection. Meanwhile, Activity theory adds a layer of understanding by considering the social and cultural contexts in which rural users operate. It examines how cultural norms, historical factors, and individual behaviors influence

cybersecurity practices and compliance within these communities. By integrating these theories, the study can develop a comprehensive cybersecurity awareness framework that not only deters potential cyberattacks but also aligns with the unique socio-cultural dynamics of rural environments. This synthesis of theories ensures that the proposed cybersecurity strategies are not only theoretically sound but also practically applicable and culturally relevant to the rural context.

2.10. Conceptual framework

According to Mishra and Alok (2022), a conceptual framework represents the researcher's perspective on the issue or concern under study and guides the direction of the research. It may be an adaptation of a model from prior research, tailored to the current inquiry. By employing a conceptual framework, the researcher illustrated the interconnections or relationships among the different constructs aimed to study, thereby indicating the study's direction.

The study incorporated underlying theories, beliefs, expectations, and assumptions from theoretical frameworks to provide a suitable structure for informing the research. Constructs and themes were identified and applied within the context of the study's focus, contributing to an understanding of the significance of cybersecurity in rural communities. This contextual understanding was aligned with the study's aim and objectives. Consequently, the study developed a conceptual framework, depicted in Figure 2.3, which included cases and examples of cybersecurity practices.

In literature, the Game, General Deterrence, and Activity theories have been recognised as highly predictive frameworks and have been widely used in various information security research (Yeng, Szekeres, Yang, and Snekkenes, 2021). Given their comprehensiveness and suitability for the study, the researcher adopted these models. The conceptual framework illustrates the relationship between the independent and dependent variables, as depicted below:

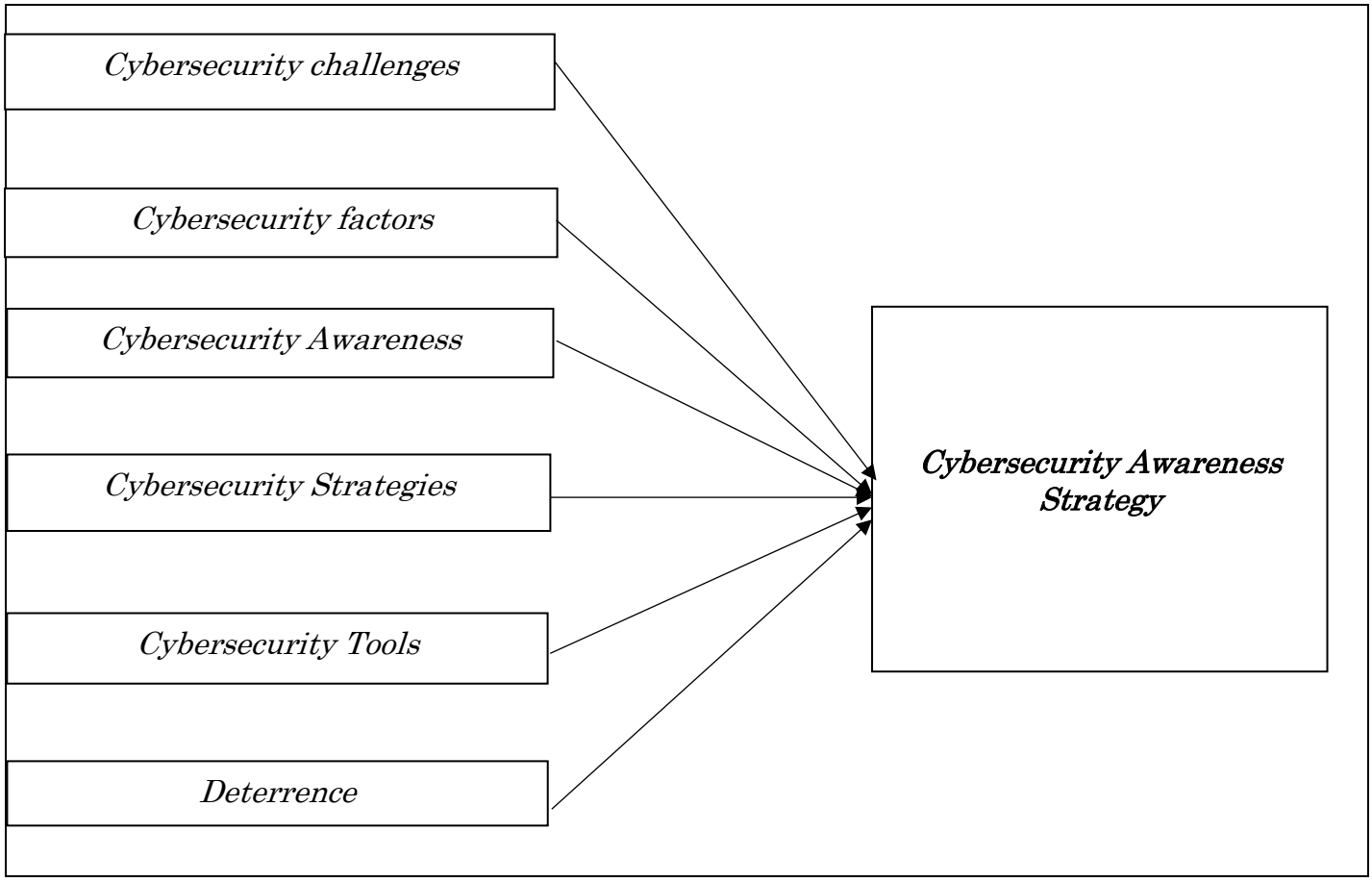

Figure 2.3: Conceptual Framework Derived from General Deterrence, Game and Activity Model (Source: Researcher – Proposed Model).

The conceptual framework integrates key elements from General Deterrence Theory, Game Theory, and Activity Theory, alongside additional constructs such as cybersecurity challenges, factors, and awareness, to create a comprehensive model for understanding and enhancing cybersecurity in rural settings. The interaction between these elements is critical to the framework's effectiveness. For instance, Cybersecurity Strategies and Tools, derived from Game Theory and Activity Theory, are not only influenced by the Cybersecurity Challenges identified in rural communities but are also shaped by the level of Cybersecurity Awareness. The Deterrence component, rooted in General Deterrence Theory, is expected to interact with Cybersecurity Factors, such as government support and community engagement, to enhance the perceived risks for potential cyber offenders. This interaction underscores the importance of a multi-layered approach, where the strategic application of deterrence measures, coupled with the appropriate tools and strategies, can effectively mitigate cybersecurity challenges in rural areas. Furthermore, the framework anticipates that higher levels of cybersecurity awareness will lead to better utilization of tools and strategies, reinforcing the overall cybersecurity posture of rural communities. By explicitly linking these constructs, the

framework not only highlights the interdependence of the theoretical elements but also provides a roadmap for addressing the unique cybersecurity needs of rural populations.

Each construct serves a specific purpose within the framework, as outlined below:

(a). Cybersecurity Challenges were measured in terms of perceived cybersecurity challenges. Previous studies (Richardson et al., 2020; Smith et al., 2023) have highlighted several cybersecurity challenges faced by rural communities, including lack of cybersecurity awareness, inadequate resources, and limited access to internet infrastructure for implementing security measures. These challenges were identified through empirical research and qualitative assessments of rural populations' cybersecurity needs.

(b). Cybersecurity Factors were assessed by evaluating factors influencing cybersecurity policies. The degree of factors that can influence cybersecurity policies was achieved by measuring government support and regulations, community engagement and awareness, availability of cybersecurity expertise, funding and resources, and collaboration with local organizations.

(c). Cybersecurity Awareness was assessed by measuring the level of awareness individuals in rural communities have regarding cybersecurity. Literature has demonstrated that targeted awareness campaigns and educational initiatives can improve cybersecurity knowledge and behavior among rural residents (Smith et al., 2023; Wang, et al., 2018). Therefore, the degree of awareness was measured in terms of opportunities and risks of cybersecurity awareness and training programs.

(d). Cybersecurity Strategies of cybersecurity awareness strategy were measured as the degree of approaches used for mitigating cyber threats and enhancing cybersecurity resilience.

(e). Cybersecurity Tools of cybersecurity awareness strategy were measured as the degree of resources available for safeguarding digital assets and mitigating cyber threats.

(f). Deterrence of cybersecurity awareness strategy was measured as the degree of deterrent measures implemented to discourage and prevent cyber threats.

Table 2.3: Summary of the theoretical frameworks and constructs that was adopted in the study.

Theory	Construct
Game Model	Strategies
General Deterrence Model	Deterrence
Activity Model	Tools

2.11. Development of Hypotheses

The theoretical reviews and the conceptual framework (Figure 2.3) led to the formulation of the following hypotheses:

- **H1:** Cybersecurity challenges influence cybersecurity awareness strategies.
- **H2:** Cybersecurity factors influence cybersecurity awareness strategies.
- **H3:** Cybersecurity awareness influences cybersecurity awareness strategies.
- **H4:** Cybersecurity strategies influence cybersecurity awareness strategies.
- **H5:** Cybersecurity tools influence cybersecurity awareness strategies.
- **H6:** Deterrence influences cybersecurity awareness strategies.

2.12. Research Gap

The available literature on cybersecurity risk management in rural communities revealed a pressing necessity; rural communities must grasp the significance of cybersecurity. Thus, the imperative for a cybersecurity awareness strategy to ensure residents' adequate protection became evident. Cybersecurity awareness was going to enable rural communities to identify threats and vulnerabilities associated with cyberspace; and therefore, apply administrative actions and comprehensive solutions. The knowledge of threats and vulnerabilities of cyberspace would enable rural communities to mitigate cyber risks and be able to implement cyber-risk management strategies. Moreover, various studies have been conducted on cybersecurity, cyberattacks, threats, and countermeasures in rural communities. However, many of those studies were not specifically addressing rural communities by implementing them with cybersecurity awareness strategy. The studies focused on large organizations with adequate resources to mitigate cybercrimes.

Therefore, this study aimed to address the research gap by conducting an in-depth investigation into the cybersecurity awareness landscape of rural communities in the Mopani District. The research aimed to contribute valuable insights by investigating existing knowledge and practices related to cybersecurity in this context. These insights can inform

the design and implementation of targeted cybersecurity awareness initiatives to protect and empower rural residents from potential cyber risks or threats.

2.13. Chapter Summary

This chapter presented a summary of recognised journals' literature models of cybersecurity concepts and challenges in rural communities. The chapter defined the term "Cybersecurity" as used by different countries. Moreover, this chapter provided rationales for the theoretical models employed and introduced a conceptual framework guiding the study. The chapter further provided a discussion of various effects, factors, and existing cybersecurity risk management frameworks, and the various cybersecurity factors. Finally, the study and knowledge gaps were identified in this chapter.

3. CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY

3.1. Introduction

Mishra and Alok (2022) assert that research methodology outlines the procedures for conducting a study, encompassing research aims and objectives, research questions, as well as data collection and analysis methods. The chapter detailed the methodology adopted in the study, encompassing aspects such as data collection, analysis, sampling methods, and ethical considerations.

3.2. Research Paradigm

A research paradigm refers to a set of common beliefs and agreements shared among researchers regarding problem understanding and resolution (Kamal, 2019). It can also be described as the framework within which theories and practices of a discipline are situated to develop a research plan (Park, Konge, and Artino, 2020). Saunders, Lewis, and Thornhill, (2019) suggest that various philosophies can guide a study. Table 3.1. adapted from Saunders et al. (2019) provides a concise comparison of other research philosophies.

Table 4.1: Comparison of the research philosophies (Adapted from Saunders, Lewis, and Thornhill, 2019).

Research Philosophy			
Positivism	**Realism**	**Pragmatism**	**Interpretivism**
This belief system (philosophy) exists externally, is based on objectivity, and remains unaffected by social influences.	This philosophy is grounded in objectivity, separate from human thoughts, beliefs, or awareness of their presence (realist perspective). Yet, it is filtered through social influences (critical realist perspective).	This philosophy is external, diverse, and selects viewpoints considered most appropriate for addressing research inquiries.	This philosophy is socially constructed, subject to change, and encompasses multiple perspectives.

After careful consideration of the above-explained philosophies, that were concluded to be appropriate in directing the collection of data, analysing the data, and then providing

conclusions. This is because the theories aligned with the objectives of the study and therefore aided the study to be conducted in a scientific manner; this is to say based on scientific and accurate data. The study was further conducted in a manner that understood that different respondents yield different perspectives; and the questionnaires were aimed at providing knowledge that is specific to the topic. These methods were all directed by the research philosophies chosen. The study followed the positivist paradigm, and the rationale is given in sub-section 3.2.1.

3.2.1 Positivist Approach.

Positivists advocate for a singular reality and seek to identify causal relationships using objective quantitative measures. This perspective often aligns with the scientific method (Creswell and Creswell, 2018), emphasising the examination of variable relationships. Researchers strive for independence to mitigate bias in inquiry processes. Knowledge generation in positivism is rooted in observing and measuring the objective reality of the world, guided by established rules or theories that require verification for comprehension (Creswell and Creswell, 2018). The traditional research process involves starting with a theory, collecting data to support or validate it, and subsequently refining it through testing and revisions (Kumar, 2018). The goal is to construct accurate, relevant, and truthful statements elucidating the issue under investigation. Objectivity is paramount, underscoring the importance of validity and reliability. In this particular study, a quantitative approach was employed for data collection and analysis. This is because the quantitative approach was suitable in providing an understanding of the research problem. This paradigm allowed for the testing of proposed framework, while yielding statistically described findings pertaining to sentiments that were associated with the larger population under study regarding cybersecurity awareness.

3.3. Research Approach

Creswell and Creswell (2018) describe a research approach as the blueprint and methods employed for conducting research, evolving from initial assumptions to detailed procedures for data collection, analysis, and interpretation. In the same study, it is stated that the choice of research approach is guided by the research problem itself (Creswell and Creswell, 2018). Three primary approaches to research are commonly recognised: Qualitative, Quantitative, and Mixed-method.

Qualitative research involves delving into and comprehending individuals' perspectives on a human issue, often relying on thematic analysis for drawing conclusions (Brink, Van der Walt, and Van Rensburg, 2018). They further stated that quantitative approach assesses objective theories by examining relationships between variables. Quantitative research uses inquiry strategies such as experiments and surveys, gathering data via predetermined instruments to

produce statistical outcomes (Creswell and Creswell, 2018; Kumar, 2018). Data collection in this approach aims to quantify information, subjected to statistical analysis to either support or refute alternative hypotheses (Saunders, et al., 2019).

The Mixed-method approach, as described by Brink, et al. (2018), involves gathering both quantitative and qualitative data, merging them, and employing diverse designs that encompass philosophical assumptions and theoretical frameworks. Creswell and Creswell (2018) further defined this approach as an organised investigation combining numerical data collection and statistical techniques with interpretative and in-depth qualitative data acquisition and management techniques.

In the present study, a quantitative research approach was adopted for data collection and analysis, given the large number of participants involved. This approach facilitated the collection of statistical data and evidence-based insights to address the study's research problem, enabling the researcher to quantify factors contributing to the rise of cybercrime in rural communities within the Mopani District.

3.4. Research Design

Research design encompasses the method, technique, and framework that steer the collection and analysis of data, and it enables researchers to establish a logical and coherent connection between empirical data, research objectives or questions, and eventual conclusions (Creswell and Creswell, 2018). Research designs, as outlined in the study, represent distinct types of inquiry within qualitative, quantitative, and mixed methods approaches, offering tailored guidance for procedures throughout a research study.

3.4.1. Research Design - Survey

The survey design is geared towards collecting data from one or multiple groups within a large population, focusing on examining the characteristics of the specific sample selected (Kumar, 2018). Its distinguishing feature lies in its utilization of a large sample size compared to other research methods and designs. In this study, primary data was gathered through survey questionnaires. The survey questionnaires allowed the study to provide insights from rural communities by finding out the thoughts, intentions, and purposes of a great number of individuals (Kumar, 2018; Creswell and Creswell, 2018). The structured questionnaire was developed to assess participants' cybersecurity challenges, factors, awareness, attitudes, and behaviors. The structured questionnaire further provided a numeric description of trends and opinions about cybersecurity from respondents of the Mopani District.

3.4.2. Questionnaire Development

The questionnaire was constructed based on the variables and constructs outlined in the Game, General Deterrence, and Activity Models, aligning with the objectives of the study. Questions were adapted, merged, and refined from previous research, drawing from studies such as those by Heidt, and Gerlach, (2019) and Nkurunziza, (2021). These studies utilised the Game, General Deterrence, and Activity models to investigate perceptions of cybersecurity, with additional objectives integrated to encompass other constructs within the conceptual framework concerning cybersecurity awareness. Questionnaire items were crafted following a comprehensive review of existing literature and validated measures pertaining to cybersecurity awareness. Each item was carefully crafted to assess participants' knowledge, attitudes or perceptions, and behaviors related to cybersecurity.

The survey questionnaire comprised various types of questions, including dichotomous questions offering two response options; either yes or no. Additionally, multiple-choice questions were included, prompting participants to select an answer from a predetermined set of options. Moreover, many questions allowed participants to choose one or more responses. Likert-type questions were also incorporated, featuring a five-point scale ranging from SD (Strongly Disagree) to SA (Strongly Agree), enabling participants to express their level of agreement or disagreement with statements. Table 3.2 illustrates the derivation of the Survey Questionnaires based on the study's objectives.

Table 3.2: Formulation of the Questionnaire

Questionnaire Design		
Dimension(s)	Variable(s)	Instrument(s)
Demographics Info	• Age • Gender • Race • Educational Level • Occupation • Years of Residence	• All Multiple-Choice
Cybersecurity Challenges		
Cybersecurity Challenges	• Experience of Cyberattacks • Type of Cyberattacks experienced • Impact of the cyberattacks • The most significant cybersecurity challenge(s)	• Dichotomous • Multiple Choice • Multiple-Choice • Multiple-Choice
Factors Influencing Cybersecurity Policies		
Factors Influencing Cybersecurity Policies	• Awareness of any local cybersecurity policies or initiatives • Type(s) of cybersecurity policies or initiatives used • Factors that influence the development and implementation of cybersecurity policies	• Dichotomous • Multiple-Choice • Multiple-Choice
Cybersecurity Awareness		

Cybersecurity Awareness	• Level of awareness of cybersecurity concepts • Frequency of seeking information for cybersecurity threats and best practices • Type(s) of cybersecurity training or education received • Level of effectiveness of the cybersecurity training or education received	• Likert-Type Questions • Multiple-Choice • Multiple-Choice • Multiple-Choice
Rural Communities' Attitude towards cybersecurity		
Rural Communities' Attitude towards cybersecurity	• Importance of cybersecurity for the safety of the community • Concern about the potential cybersecurity threats • Education about cybersecurity • Investment in cybersecurity measures and tools • Level of awareness about cybersecurity	• Likert-Type Questions • Multiple-Choice
Cybersecurity Strategies (Construct)		
Strategies of Cybersecurity	• Sources used for Cybersecurity • Usage of strong, unique passwords for online accounts • The frequency of updating software and applications to the latest versions	• All Multiple-Choice

	• The level of caution exercised when clicking on links or attachments in emails from unknown senders	
Cybersecurity Tools (Construct)		
Tools for Cybersecurity	• Usage of antivirus or anti-malware software on devices • Type(s) of firewall protection used on home network • Awareness of the use of encryption to secure data on devices • Availability of cybersecurity tools • Awareness of any cybersecurity strategies or tools used to enhance online security • Awareness of cybersecurity strategies or tools • Level of cybersecurity tools accessibility to community members	• Dichotomous • Multiple-Choice • Dichotomous • Dichotomous • Dichotomous • Multiple-Choice • Multiple-Choice
Cybersecurity Deterrence (Construct)		
Deterrence	• Perceived effectiveness of cybersecurity measures in deterring cybercriminal activities • Perceived effectiveness of additional cybersecurity measures as deterrents to cybercriminal activities	• Likert-Type Questions • Multiple-Choice

3.5. Study Population

A population refers to the complete set of individuals of interest to the researcher (Brink et al., 2018). As noted by Mabaso and Kumar (2018), a study's target population represents the specific group of individuals from whom the researcher seeks to acquire knowledge and make inferences. This target population encompasses the entire collection of elements that the researcher aims to generalise findings to (Brink et al., 2018). In the context of this study, the population consisted of individuals residing in the Mopani District. Specifically, the target population comprised internet users residing in the rural areas of Ba-Phalaborwa Municipality.

3.6. Description of the Study Area

The study area encompassed rural villages within the Ba-Phalaborwa Municipality of the Mopani District. As indicated in the Ba-Phalaborwa Municipality Draft Integrated Development Plan (IDP) for 2021-2022, the Phalaborwa area serves as a notable example of population densification, with approximately 94% of the municipal population residing within or near a 15km radius of the Phalaborwa urban complex. Within this, Phalaborwa town accommodates around 20% of the population, while the remaining 31% constitutes the rural population. The remaining 6% includes populations from areas such as Gravelotte, Grietjie, and Selwane. Over the years, the population of the Ba-Phalaborwa Municipality has shown growth, increasing from 131,089 according to the South African Statistics Census 2011, to 150,637, and subsequently to 168,937 based on the Community Survey of 2016. This growth has been accompanied by an increase in the number of households, reaching 49,100 (Ba-Phalaborwa Municipality Draft IDP, 2021-2022).

3.7. Sample, Sampling Techniques and Sampling Size

A sample comprises a group of individuals chosen from within a population (Brink et al., 2018). The same study further states that sampling is the method of selecting a portion of a population to represent the whole, whereas a study conducted by Saunders, et al. (2019) elaborate on sampling as a statistical process employed to select a subset of the population of interest, enabling statistical inferences and observations about the entire population.

3.7.1. Multi-stage sampling technique

The number of individuals that are internet users and those that are not internet-users is unknown in the Mopani District. For this reason, a multi-stage sampling technique was used in this study. Multi-stage sampling is a technique employed when there is no comprehensive list of all members of the population available (Kumar, 2018).

The multiple stages of sampling involved in this study:

a) the random selection of streets and villages that were considered as primary units.
b) the identification of individuals who meet the qualities to be the initial participants.

These potential initial respondents were considered as the secondary units.

3.7.1.1. Selection of primary units

The study employed a simple random technique to select the primary units of analysis. In this technique, the selection of one respondent does not influence the selection of another. Simple random sampling is often employed when there is limited prior knowledge about the population (Creswell and Creswell, 2018). The study's primary units were obtained from the areas around Ba-Phalaborwa in the Mopani district. Participants, which were internet users, were obtained from streets, community clusters, complexes, schools, government offices, and malls which were randomly selected. The Ba-Phalaborwa Municipality villages included in this study were Majeje, Humulani, Mashishimale, Selwane and Ninakhulu.

3.7.1.2. Selection of secondary units

The non-probability snowballing, and convenience sampling were used when sampling participants to be considered as the secondary units. Convenience sampling entails recruiting readily available participants for the study, typically individuals who meet the criteria and are willing to participate (Kumar, 2018). Snowball sampling, as described by Brink et al. (2018), involves enlisted participants aiding in the recruitment of additional participants, particularly in scenarios where access to the population is challenging for the researcher. In this instance, the referral method was utilised to recruit a sufficient number of participants for the study.

3.7.2. Sample Size of the Study

As stated by Creswell and Creswell (2018), determining the optimal sample size is a crucial step in the research process. The quality of the sample, and to some extent the survey, is influenced by the sampling frame (Kumar, 2018). The sampling frame serves as a comprehensive list of elements intended for sampling within the target population (Creswell and Creswell, 2018). Selecting a high-quality sampling frame that is appropriate for both the population being studied and the data collection method is a crucial step in any study. However, determining a sample size is not always easy because it is dependent on the type of study being conducted. For this study, there was no definite population of internet-users, therefore, the study population was considered hidden. Considering the unknown population of internet-users, Cochran's formula (Nanjundeswaraswamy and Divakar, 2021) was employed to determine the sample size of the study.

Cochran's for unknown population

$№= z^2\ pq/e^2$

The researcher assumed that the population size was unknown. The formula developed by Cochran in 1963 was employed in the study to calculate the sample size, assuming maximum variability at 50% (p = 0.5), and considering a 95% confidence level with a precision of ±5%. The calculation for the required sample size is as follows:

p = 0.5 and hence **q** =1-0.5 = 0.5; **e** = 0.05; **z** =1.96.

N= 384

A minimum of 200 participants was targeted to ensure adequate power for detecting significant effects in the statistical tests, following Cohen's (1988) effect size conventions. This sample size is sufficient to achieve reliable results and validate the study's hypotheses.

3.8. Dependent and Independent Variables, and Hypotheses Testing.

The variables (dependent and independent) were defined to guide the research study.

3.8.1. Dependent Variables - These are the outcome variables that are measured in the study and are expected to change (Creswell and Creswell, 2018). In this study, dependent variables include cybersecurity challenges, policies, factors, attitudes, strategies, tools and deterrence.

3.8.2. Independent Variables - In the context of this study, the independent variable is the development or implementation of a cybersecurity awareness strategy. This variable, as defined by Creswell and Creswell (2018), is controlled or manipulated by the researcher and is anticipated to influence the dependent variables.

3.8.3. Hypotheses Testing - Given the research questions and variables, the following hypotheses were tested:

- **H1:** Cybersecurity challenges influence cybersecurity awareness strategies.
- **H2:** Cybersecurity factors influence cybersecurity awareness strategies.
- **H3:** Cybersecurity awareness influences cybersecurity awareness strategies.
- **H4:** Cybersecurity strategies influence cybersecurity awareness strategies.
- **H5:** Cybersecurity tools influence cybersecurity awareness strategies.
- **H6:** Deterrence influences cybersecurity awareness strategies.

3.9. Inclusion and exclusion criteria

The criteria are described in subsections 3.81 to 3.8.2.

3.9.1. Inclusion

The study only included rural communities (rural areas) of the Ba-Phalaborwa area. Rural communities were selected in this regard because they are regarded as being more vulnerable to cyberattacks (Mashiane et al., 2019). Specifically, internet-users in the rural communities of Ba-Phalaborwa were included in the study. This is because cybersecurity awareness directly affects people that use the internet.

3.9.2. Exclusion criteria

The study excluded cities, towns, and townships of Ba-Phalaborwa. Non-internet users were also excluded from the study. The study used a questionnaire that entailed questions able to identify if a person is an internet user or not. Therefore, non-internet users were identified through their responses on the questionnaire.

3.10. Data collection procedure

Questionnaires were used to collect data. These questionnaires were distributed to members of the community clusters, villages, groups, streets, and housing units around those rural communities of Ba-Phalaborwa. The questionnaire was structured into eight distinct sections. Section A: Demographic information; section B: Cybersecurity challenges faced by rural communities in the Mopani District; section C: Factors that influence cybersecurity policy; section D: Cybersecurity awareness; section E: Cybersecurity attitude; section F: Cybersecurity strategies used in rural communities (Strategies construct); section G: Disincentives (Deterrence construct); section H: Cybersecurity tools used by rural communities of the Mopani District (Tools construct).

3.11. Analytical framework

Table 3.2 outlines the analytical framework based on which this study undertook model testing. As expressed in Table 2.3, the tenets of the above-discussed frameworks (sections 2.10) were used as referencing point for the proposed model in this study. Analytical framework deals with the management and organization of data, through codes or themes that can be set as categories. These categories are then used as the basis for analysing the data (Osman, 2019). Therefore, analytical framework directs conclusions and recommendations from the findings of the study.

Table 5.2: Analytical framework

Study Construct	Theory	Theoretical Assumption/ (Independent variables)	Dependent variables	Supporting Documents
Strategies	Game theory	Cybersecurity strategies	Cybersecurity Awareness Strategy	Professor Gabriel Kabanda (2018)
				Samuel Waithaka (2014)
Deterrence	General Deterrence theory	Disincentives		
Tools	Activity theory	Cybersecurity tools		

3.12. Data Analysis

Brink et al. (2018) define data analysis as the process of reasoning to comprehend gathered data, aimed at describing and illustrating patterns while evaluating the specifics of the investigated data. In the study, data was analysed using descriptive statistics to summarise participants' demographic characteristics and cybersecurity-related variables. Specifically, correlation and regression analyses were employed to explore relationships between independent and dependent variables. The Pearson's correlation coefficient (Pearson's r) was adopted to assess the strength and direction of the linear relationship between the independent and dependent variables. Pearson's r was chosen due to its suitability for continuous data and its widespread use in social science research (Cohen, 1988). Furthermore, simple linear regression was employed to examine the predictive relationship between the independent variables and the dependent variable. This method was selected for its effectiveness in analysing the relationship between a single independent variable and a dependent variable, allowing for clear interpretation and understanding of the data. SPSS (Statistical Package for the Social Sciences) was used for all statistical analyses, enabling the generation of both inferential and descriptive statistics. The objective of the analysis was to address the research questions and achieve the study's objectives by determining the relationships and significance between the variables.

3.13. Ethical issues or consideration

Ethical consideration entails the researcher's responsibility to honor the rights, needs, values, and desires of the participants (Creswell and Creswell, 2018). This study adhered to the University of Venda's (UNIVEN) Ethical Considerations concerning interactions with human subjects. Ethical clearance was obtained from the Research Office of the University of Venda. Data will be securely retained for five years. Additionally, a gatekeeper's letter granting permission to conduct the study was obtained from the University of Venda Research Office.

3.13.1 Informed Consent

In the study, participants were fully briefed on the study's objectives and the proposed methodology. The researcher disclosed their affiliation with the university to establish credibility. Participants were assured of their right to withdraw from the study at any point without facing penalties. It was made clear that participation was entirely voluntary, and no compensation would be provided. Before giving consent, participants were encouraged to ask any questions they had. Upon agreement, participants were presented with an informed consent form, which they signed to indicate their understanding and agreement with the study's terms.

3.13.2 Anonymity

Anonymity, as an ethical principle, ensures that neither the researcher nor anyone else can identify the participants once data collection is completed (Creswell and Creswell, 2018). This study strictly adhered to the principle of anonymity by assigning pseudonyms to participants for identification purposes.

3.13.3 Privacy

Creswell and Creswell (2018) defined privacy as actions that prevent other individuals either than the participant to observe or analyse. In this study, participants were allowed and given their right to privacy. The distributed questionnaires were also self-administered, so the participants completed them in their own spaces. The information from the participants was given anonymously; this was done to ensure the participants' privacy

3.13.4 Confidentiality

Confidentiality entails the handling of information in a manner that ensures its privacy; it can be viewed as an extension of privacy (Kumar, 2018). In this study, agreements were established between the researcher and the participants, including the assurance of non-disclosure of participants' names, thereby upholding confidentiality.

3.14. Pilot Study

According to Mishra and Alok (2022), pilot studies serve as preliminary investigations designed to assess the feasibility of critical components within a larger study, typically a randomised controlled trial. They help anticipate an appropriate sample size for the full-scale research and refine various aspects of the study design (Kumar, 2018). Given that randomised controlled trials often require substantial financial and time commitments, researchers must ensure confidence in essential procedures to avoid wasting resources.

In this study, a pre-test was conducted by distributing the questionnaire to a small group of secondary school learners and teachers in rural areas. The pre-test served several purposes, including identifying errors in the questionnaire, assessing its clarity and length, and refining the arrangement of questions to avoid biasing participant responses. Based on the feedback obtained from the pre-test, several specific changes were made;

- Error correction - the researcher corrected unclear terms such as "DDoS attack, Malware infection, Ransom attack, Phishing, and Data breach" by adding a brief explanation.
- Clarity and length - the researcher simplified questions in Sections A and B to avoid confusion, e.g., the researcher clarified the wording of "Cybersecurity Challenges" for better understanding.
- Question arrangement - the researcher reordered questions in Sections C and D to group similar topics together, enhancing the logical flow and reducing potential response bias.
- Elimination of questions - the researcher removed overly technical questions, such as those asking about specific encryption methods, which were deemed too complex for the target population.

3.15. Validity and Reliability

The survey questionnaires utilised in the study were designed with the aim of obtaining reliable and valid measurements. This approach was crucial for establishing the credibility and accuracy of the study's findings.

3.15.1. Validity

Validity refers to the extent to which a research tool accurately measures the intended variable. It assesses whether the measuring instrument is suitable and appropriate for collecting the required data (Brink, Van der Walt, and Van Rensburg, 2018). Saunders, et al.,

(2019) alluded that if the techniques are transparent, they offer a compelling argument for the legitimacy of the interpretation of the results.

In this study, the questionnaire was pre-tested to assess its content validity. The exploratory factor analysis statistical test was employed to evaluate the validity of the questionnaire, ensuring that the included variables were sufficient for addressing the research questions. Additionally, the questionnaire was reviewed by the supervisors of the study to obtain feedback on the questions and their arrangement. This process helped to enhance the questionnaire's content validity and overall quality.

3.15.2. Reliability

Reliability refers to the extent to which study findings may be replicated under the same circumstances and produce similar results over time (Creswell and Creswell, 2018). According to Kumar (2018), reliability in quantitative research is mainly concerned and focus with the consistency and stability of the data gathered. Stability is the degree to which consistent findings are obtained after completing the questionnaire twice (Creswell and Creswell, 2018). To ascertain the questionnaire's reliability for the study, a pilot study was undertaken involving a small subset of participants. This step was considered to address any possible questionnaire flaws prior to its distribution to the broader sample. Cronbach's alpha coefficient was calculated to assess internal consistency, and inter-rater reliability was examined for open-ended questions.

3.16. Chapter summary

This chapter discussed the research paradigm employed in the study to answer research questions. The study used a positivist approach as its analysis paradigm; and questionnaires were used to collect data. This chapter detailed the methodology used in the study, this included the sampling techniques, sampling frame, and population of the study. The outline of data analysis was also included in this chapter. Additionally, the exclusion and inclusion criteria used when selecting participants for the study are highlighted. A layout of the pilot study and pre-test is included in this chapter. The chapter also outlined the hypotheses developed based on the reviewed theoretical literature of the study and dealt with the analytical framework. Moreover, the ethical consideration followed when dealing with participants during data collection was clearly explained in this chapter. The chapter also included the tests used in testing the validity and reliability of the measurement instrument (Questionnaire).

4. CHAPTER04: DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

4.1. Introduction

This chapter presents the findings of the study. The results were obtained from analysing data collected from the rural communities of the Mopani District. The presentation of finding aligns with the objectives of the study and is directly structured based on the theoretical framework and constructs adopted in the study (Table 2.3). Furthermore, tables and graphs were used to present the findings of the study.

The following research questions acted as guiding principles, guiding the research on various dimensions of cybersecurity awareness within the Mopani District. The research questions were formulated after conducting an extensive literature review. The literature helped the researcher to identify a gap in understanding specific challenges faced by rural communities in adopting cybersecurity measures. The research questions also addressed the aspects of the research objectives through identifying the cybersecurity challenges faced by the rural communities of Mopani, determining factors that influence cybersecurity policies, and determining the levels of cybersecurity awareness within the communities of Mopani District and identifying the attitude of the rural communities towards cybersecurity. The following were the research questions;

- *What are the cybersecurity challenges faced by rural communities in Mopani? – This research question was formulated to investigate cybersecurity threats, vulnerabilities, and obstacles encountered by the residents of Mopani, forming to understand the cybersecurity challenges at hand.*
- *What are the factors influencing cybersecurity policies in the rural communities of Mopani District? – This research question identified factors shaping the formulation of cybersecurity policies within the rural areas of Mopani.*
- *What is the level of cybersecurity awareness among rural communities in the Mopani District of Limpopo Province? – This research question assessed the levels of cybersecurity awareness within the communities of Mopani. It assisted the researcher to discover the challenges of digital literacy, knowledge, and perceptions concerning cybersecurity.*
- *What is the attitude of rural communities of the Mopani District towards cybersecurity? –This research question explored the perceptions, and behavioral patterns that defined the community's stance towards cybersecurity.*

4.2. Challenges Experienced During the Data Collection Process

The data collection process is a critical phase in any research endeavour, and despite meticulous planning, researchers often encounter challenges that can impact the quality and efficiency of data acquisition (Akhtar, 2021). In this study, several challenges were encountered during the data collection process, and it is essential to highlight and address these issues to ensure transparency and reliability in the research findings.

4.2.1. Types of Challenges Encountered

Several challenges were encountered during the data collection process. Some respondents proved challenging to reach (unavailable), citing work commitments, personal engagements, and a reluctance to participate. This introduced a potential sampling bias, which has been duly considered in the subsequent analysis. Noteworthy instances of incomplete and inaccurate information were observed, potentially stemming from unintentional errors or a lack of comprehension of the questions, thereby impacting the reliability of the collected data. Language differences and communication barriers occasionally emerged, particularly in diverse communities, potentially leading to misinterpretation of questions or responses and affecting the overall accuracy of the data. Respondents also exhibited survey fatigue, due to the lengthy survey, potentially resulting in rushed and disengaged responses that could influence the overall data quality. Additionally, the constrained time frame for data collection affected the attainment of the desired sample size, and the rushed nature of data collection might have compromised thoroughness, leading to potential oversights. Lastly, since the study covered large geographic areas, logistical challenges related to transportation, lodging, and field team coordination were encountered.

4.3. Data Screening

Out of the identified 200 potential respondents within the targeted population, communication was established for the distribution of questionnaires. All 200 questionnaires distributed were subsequently returned, rendering them viable for inclusion in the data analysis. Furthermore, during the sampling process, approximately 20 or more community residents initially declined to participate. In response to this, the reluctant respondents were successfully substituted with other willing participants to ensure the completion and representativeness of the sample.

4.4. Response Rate

Two hundred questionnaires were disseminated across five communities of Ba-Phalaborwa. The overall response rate for the survey averaged 100%, signifying a comprehensive and representative engagement with the entire population. This targeted response rate was successfully achieved through the collaborative support and efforts of the five designated

communities. Table 4.1 provides a detailed breakdown, illustrating both the actual number of questionnaires distributed to each community and the corresponding number of questionnaires that were returned.

Table 4.1: ***Survey Response Rate (N=200).***

Rural Community	Number of Questionnaires Distributed	Number of Questionnaires Collected (Returned)	Survey Response Rate (%)
Majeje Benfarm	40	40	100
Humulani	40	40	100
Selwane	40	40	100
Makhushane	40	40	100
Mashishimale	40	40	100
	200	*200*	*100%*

4.5. SECTION A: DEMOGRAPHIC INFORMATION

The acquisition of demographic information from respondents residing in the rural communities of the Mopani District was conducted through a rigorous questionnaire-based survey. This demographic data encompassed crucial parameters such as age, educational level, occupation, and the duration of residency within the Mopani District. It is imperative to note that the study aspired to attain a sample size of N=200, indicating a comprehensive coverage of all targeted respondents. The attainment of responses from the entire sample size underscores the robustness of the data collection process and enhances the reliability and representativeness of the demographic insights derived from this study, hence, these insights are crucial for understanding the diverse composition of the sample and the potential implications for various aspects of interest.

4.5.1. Age of respondents

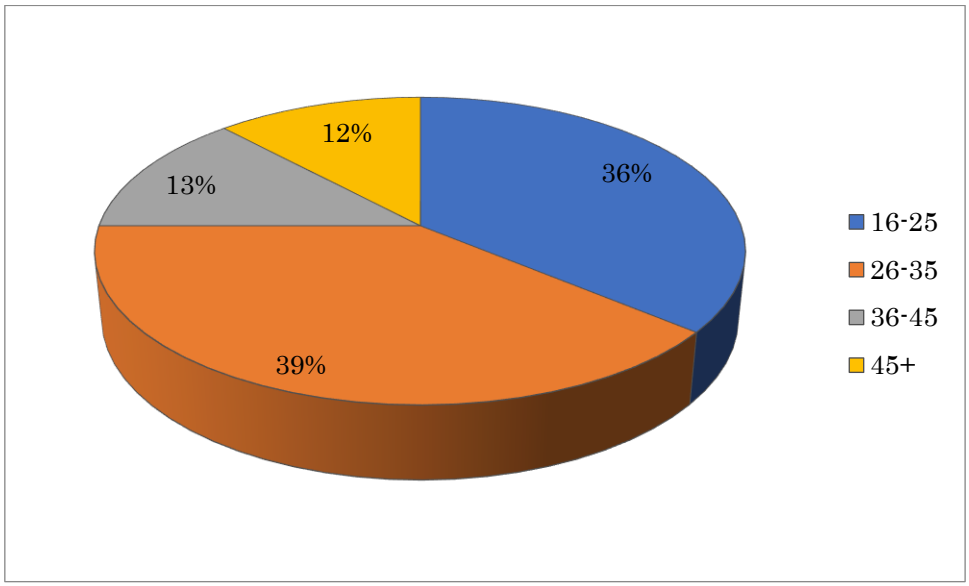

Figure 4.1: Age of respondents

Figure 4.1 depicts the age distribution of respondents, with the predominant age group falling within 26-35 years, representing 39% of the sample. This age group's predominance may reflect the high level of technological engagement and career stage, potentially influencing their familiarity with cybersecurity practices and challenges. In contrast, the younger cohort (16-25 years) constitutes 36% of the respondents, which might suggest a growing exposure to digital environments but possibly less experience with cybersecurity issues. The smaller proportions of older age groups (36-45 years at 13% and 45+ years at 12%) might indicate less engagement with current digital trends, possibly impacting their awareness and attitudes towards cybersecurity.

Understanding the age distribution can help tailor cybersecurity awareness strategies. For instance, targeted interventions could focus on younger and middle-aged adults who are more engaged with technology and might benefit from advanced cybersecurity training, while adapting strategies to address the specific needs of less represented older groups.

4.5.2. Gender of respondents

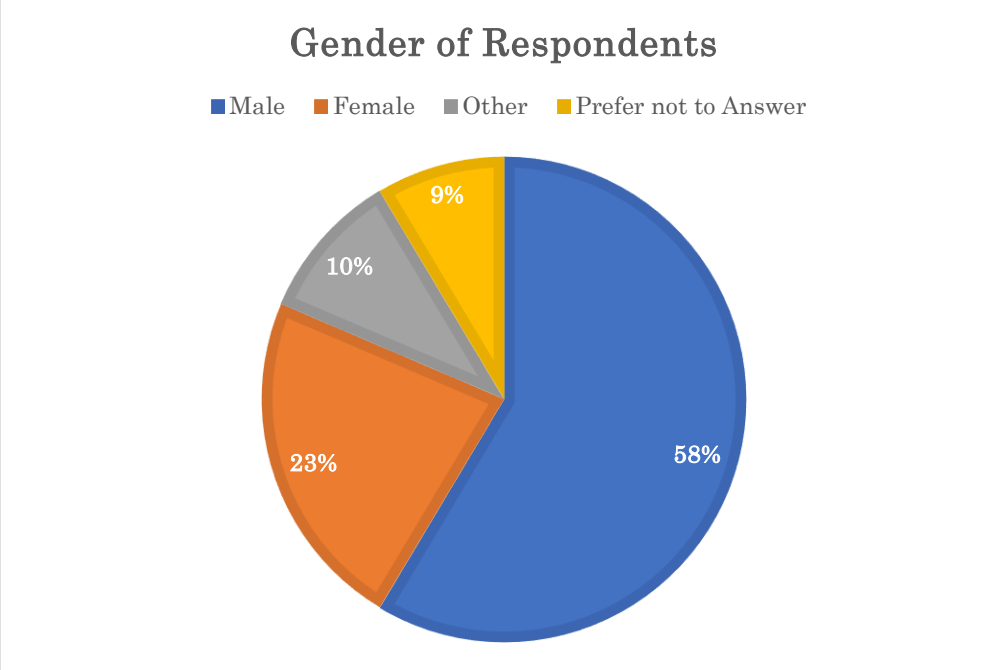

Figure 4.2: Gender of respondents

The data presented in Figure 4.2 reveals a significant gender imbalance among survey respondents in the cybersecurity field. Notably, 58% identify as male, while female representation stands at 23%. The Other category constitutes 10%, possibly encompassing non-binary gender identifications. Additionally, 9% preferred not to disclose their gender. These statistics underscore potential gender-related considerations in cybersecurity research, highlighting a need for greater inclusivity and diversity. Addressing these imbalances is crucial for fostering equal opportunities and harnessing a broader range of perspectives within the cybersecurity sector.

4.5.3. Race of respondents

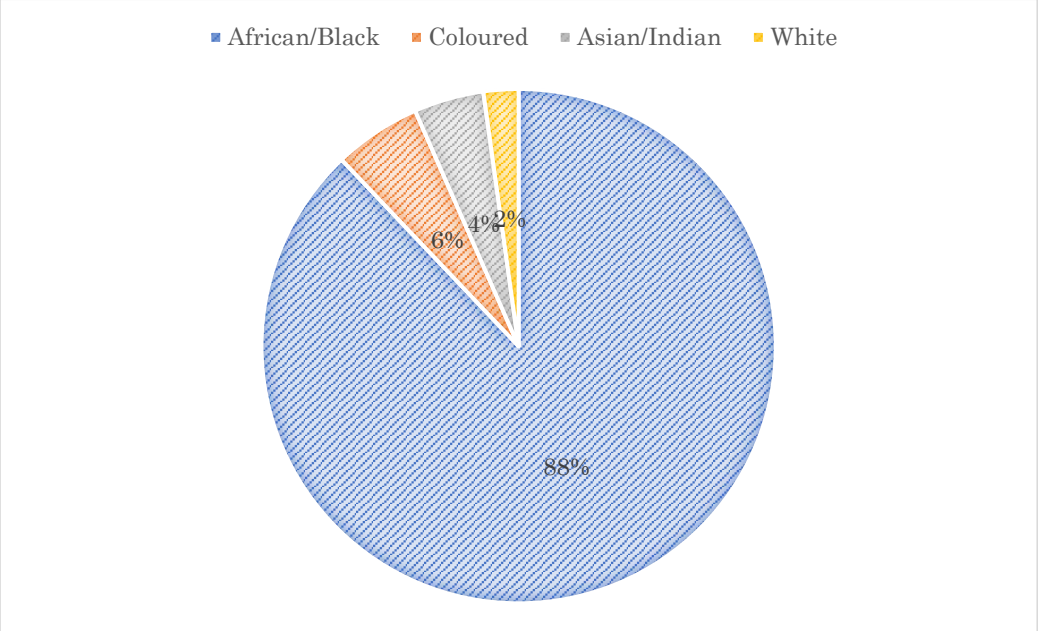

Figure 4.3: Respondents' Race

The findings from Figure 4.3 emphasise a predominant demographic composition among the survey respondents. Specifically, 88% identify as African/Black, 6% as Coloured, 4% as Asian/Indian, and 2% as White. This suggests a notable overrepresentation of the African demographic in the surveyed population. The results underscore the necessity for future research to delve into cybersecurity perceptions across diverse racial backgrounds. Understanding varied perspectives within different racial groups is crucial for developing inclusive and comprehensive approaches to cybersecurity, ensuring that strategies and policies consider the nuances of a broad spectrum of individuals.

4.5.4 Educational level of respondents

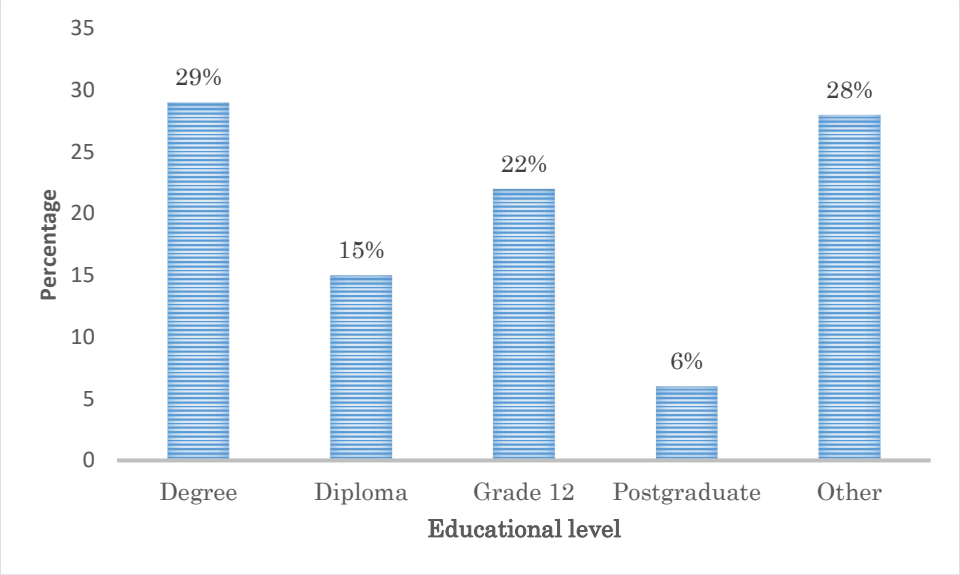

Figure 4.4: Educational level of respondents

The outcomes delineated in Figure 4.2 shed light on the educational attainment of respondents within the study. Notably, 29% of the respondents held a Degree, signifying the highest proportion among the educational categories. Following closely, 22% possessed a matriculation (Grade 12) certificate, while 15% held a Diploma. A notable 6% indicated possession of a Postgraduate Degree. Intriguingly, 28% of respondents reported having an alternative educational background. Further exploration revealed that this subset had not reached or completed Grade 12, with their highest educational level being Grade 11 and below. This collective analysis underscores a noteworthy observation where a majority of the respondents have undergone some level of formal education. The prevalence of Degree holders suggests a higher educational attainment within the surveyed population. However, the diversity of educational backgrounds, including those who did not complete Grade 12, underscores the importance of considering a broad spectrum of educational experiences within the context of the study.

4.5.5 Occupation

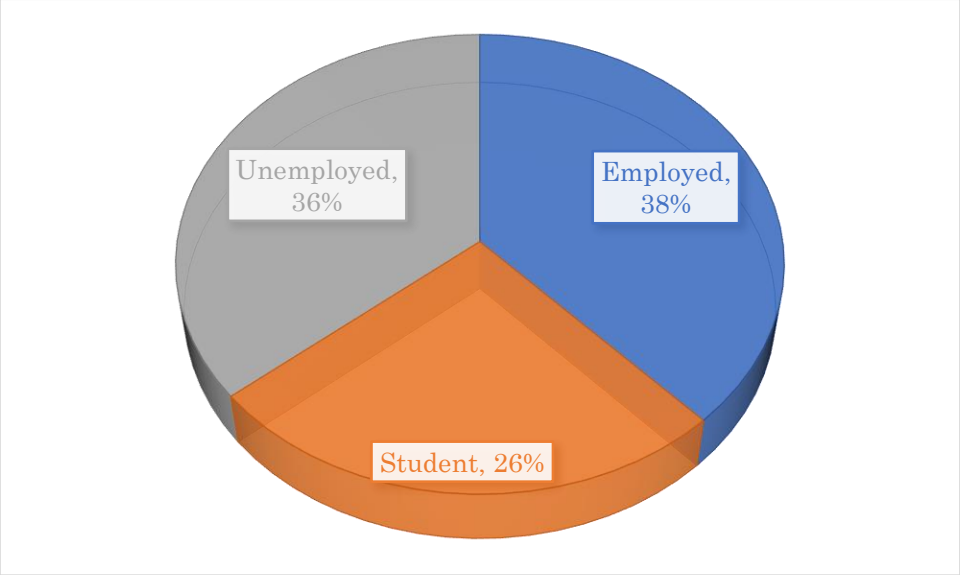

Figure 4.5: Occupation of respondents

Figure 4.5 indicates the occupational distribution among the respondents, categorising them into employed, unemployed, and student groups. The findings elucidate a diverse occupational landscape within the Mopani District. Notably, 38% of respondents identify as employed, underscoring a substantial portion of the population actively participating in the workforce. Conversely, 36% of respondents fall within the unemployed category, reflecting a comparable percentage of individuals currently not engaged in formal employment. Furthermore, 26% of respondents classify themselves as students, indicating a significant proportion pursuing academic endeavours.

This distribution reveals a dynamic and varied occupational structure within the Mopani District, where the percentages of employed and unemployed respondents exhibit a notable balance. This nuanced insight into the occupational composition contributes to a comprehensive understanding of the economic and educational dynamics within the surveyed population.

4.5.6 Years of residence in the Mopani District

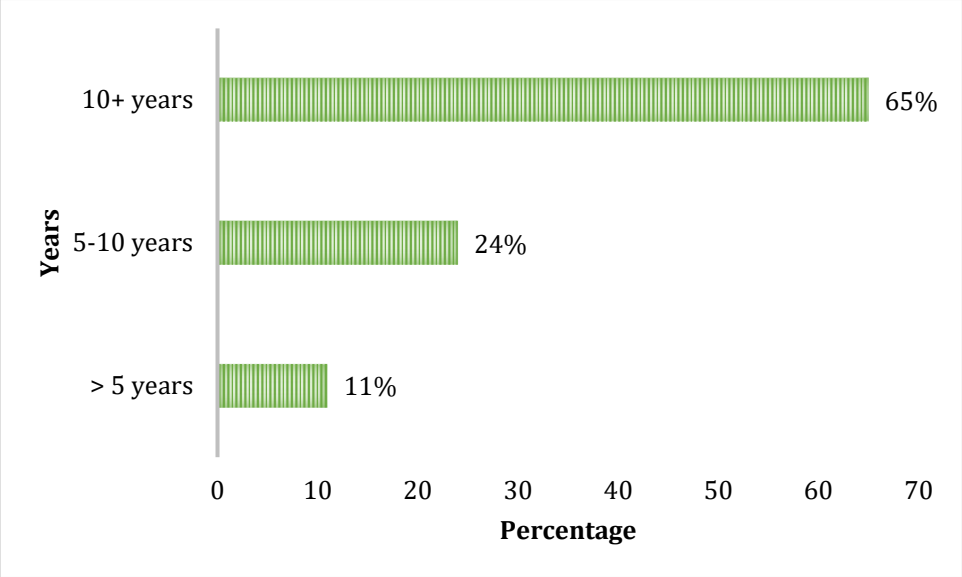

Figure 4.6: Respondent's years of residence in the Mopani District

Figure 4.6 provides an insightful depiction of the respondents' duration of residence in the Mopani District. The results reveal a significant trend, with 65% of respondents indicating a residence duration of more than 10 years. Subsequently, 24% of respondents reported a residence duration ranging from 5 to 10 years, while 11% have been residing in the district for less than 5 years. These findings suggest a noteworthy pattern of long-term residency among the majority of respondents, implying a substantial familiarity with the Mopani District. The extended duration of residence may potentially correlate with an in-depth understanding of the local landscape, including policies implemented by local governance, as well as prevalent behaviors and attitudes among the district's residents. This nuanced perspective on the respondents' tenure in the Mopani District contributes valuable context to the study, offering insights into the potential influence of local knowledge and experience on perceptions and behaviors.

4.6. SECTION B: CYBERSECURITY CHALLENGES

In this section, the researcher explored the domain of cybersecurity challenges faced by individuals and communities within the Mopani District. The aim was to gain profound insights into the firsthand experiences of residents regarding cyberattacks and the broader challenges associated with cybersecurity in the region. To extract valuable information, the researcher designed specific research questions targeting the direct encounters of participants with cyberattacks. Participants were asked whether they themselves or someone they knew had faced a cyberattack. In cases of affirmative responses, participants were further prompted to provide details on the type(s) of cyberattacks experienced. This detailed inquiry helped in categorising and understanding the nature and prevalence of cyber threats within the Mopani District.

Furthermore, the impact of these cyberattacks on affected systems or networks was thoroughly explored, encompassing dimensions such as data loss, financial implications, service disruptions, and the compromise of personal information. By dissecting the aftermath of cyber incidents, the researcher aimed to discern the tangible repercussions experienced by the community members. Moreover, the researcher sought the opinions of respondents on what they perceive as the most significant cybersecurity challenges confronting rural communities in the Mopani District. The provided options cover a wide spectrum of potential issues, ranging from the lack of cybersecurity awareness and limited access to resources to the presence of cybercriminal activities and deficiencies in cybersecurity training and policies. This exhaustive investigation ensured a comprehensive understanding of the multifaceted challenges that contribute to the cybersecurity landscape in the Mopani District.

4.6.1. Aspects of cybersecurity Awareness and Challenges in the Mopani District

The questions aligning to the objectives of the study were analysed using descriptive statistics. Therefore, percentages, mean, standard deviation were used where it was relevant and deemed fit. The questions answered are as follows:

4.6.1.1. What are the cybersecurity challenges faced by rural communities in the Mopani District in the Limpopo Province?

Several questions were raised to gain better understanding of the cybersecurity challenges faced in the rural communities of the Mopani District; amongst these are:

4.6.1.2. Have you /someone experienced cyberattack?

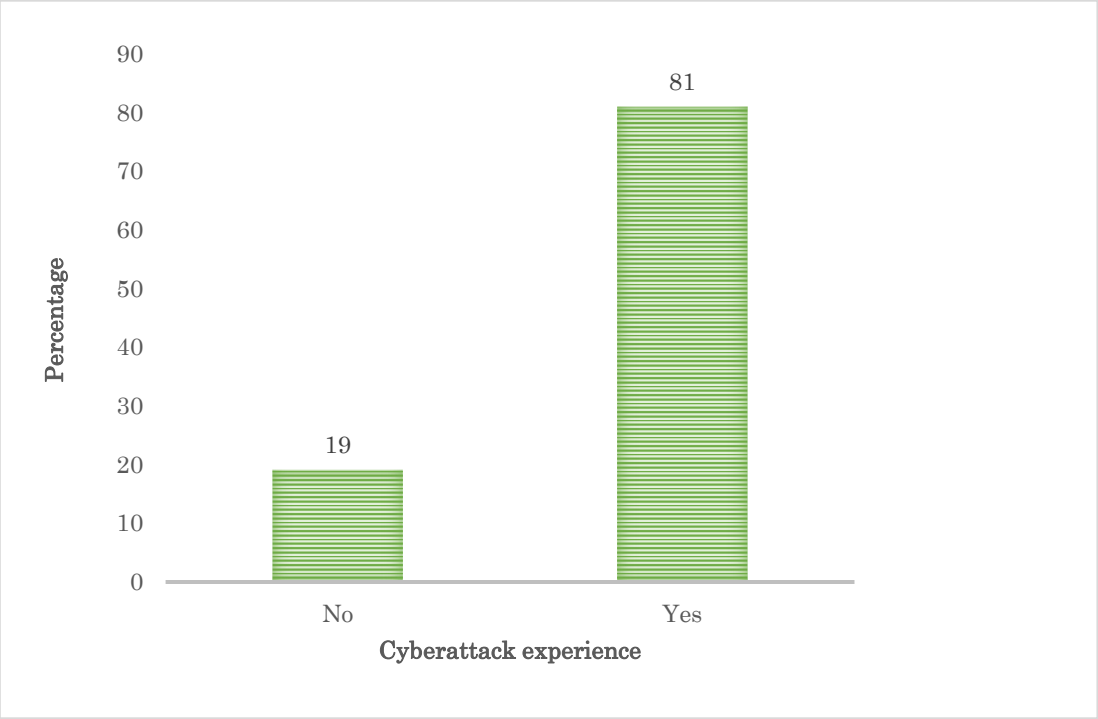

Figure 4.7: The respondents experience of cyberattack

Figure 4.7 reveals that 81% of respondents reported experiencing a cyberattack or knowing someone who has. This high percentage underscores a significant exposure to cyber threats within the community. The implication of this finding highlights the urgent need for robust and community-specific cybersecurity measures. Enhanced educational programs and preventative measures should be prioritised to address the high rate of cyberattack experiences and improve overall cybersecurity awareness in the community.

4.6.1.3. If yes, select the type of cyberattack(s) experienced

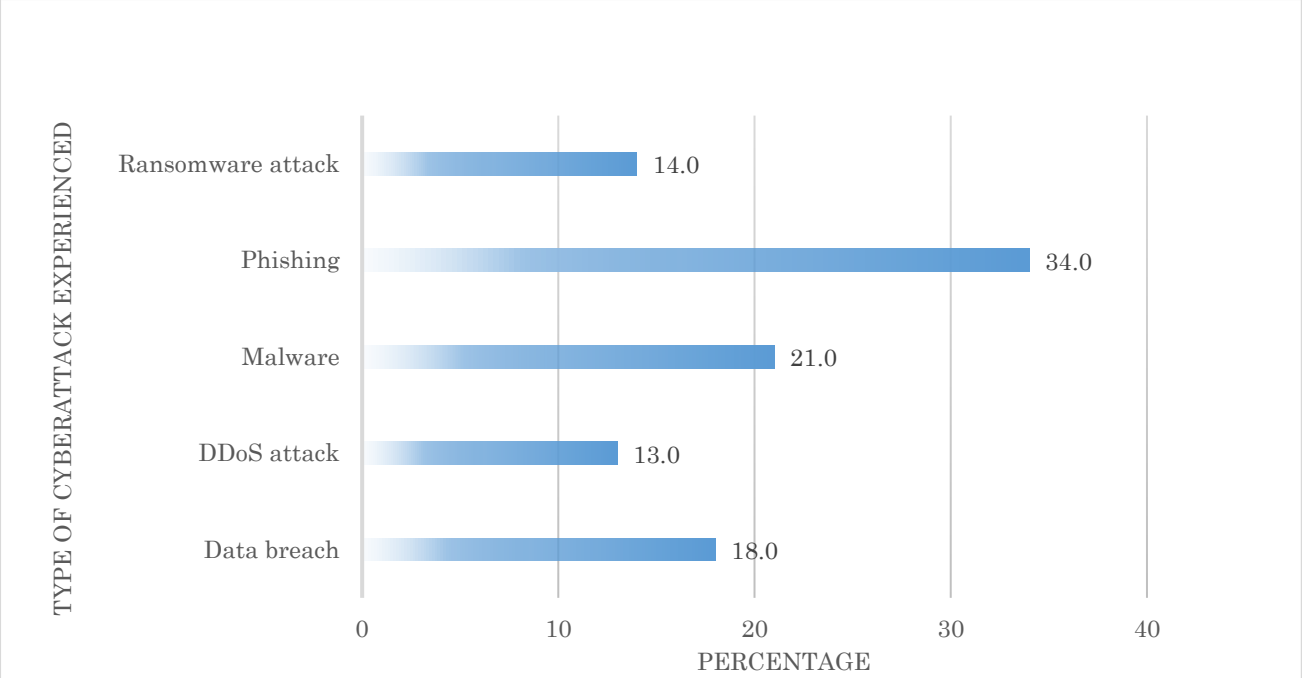

Figure 4.8: Type of cyberattack experienced by the respondents

The analysis of results (Figure 4.8) reveals that among respondents who had encountered a cyberattack, phishing was the most prevalent, constituting 34% of reported incidents. Following closely was malware at 21%, followed by data breach at 18%, ransomware attacks at 14%, and DDoS attacks at 13%. These findings underscore the existence of cyberattacks within the Mopani District, signifying a notable challenge. Particularly noteworthy is the prevalence of phishing attacks, emerging as the predominant type of cyberattack experienced by the respondents. This insight underscores the urgency of addressing and mitigating cybersecurity threats in the Mopani District, with a specific focus on phishing vulnerabilities.

4.6.1.4. What was the impact of the cyberattack(s) on your or the person's affected system/network?

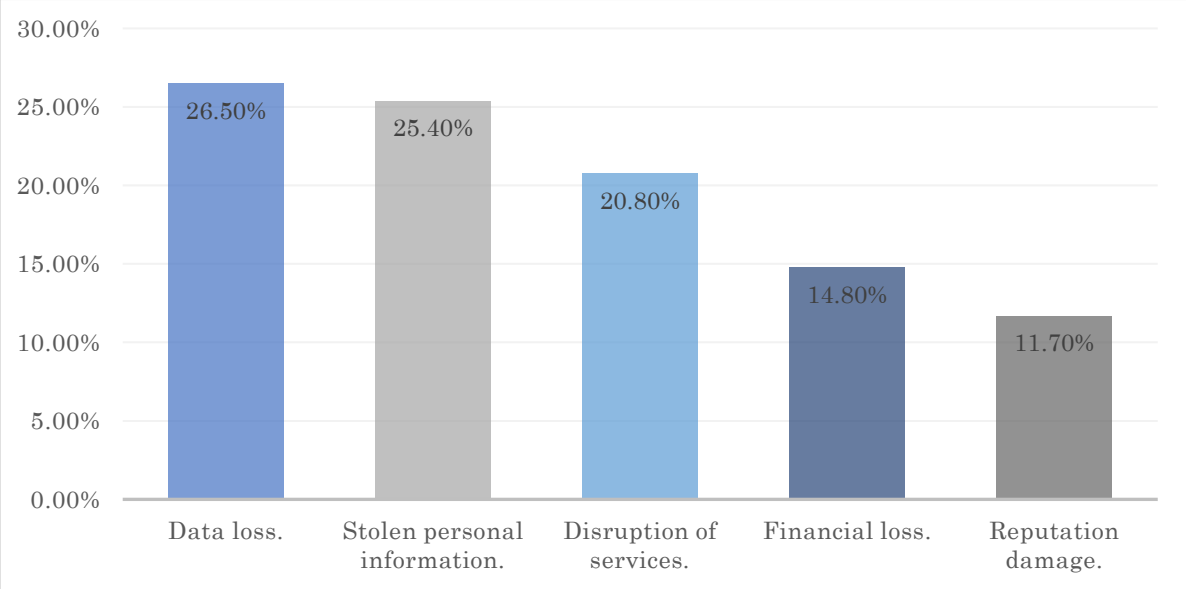

Figure 4.9: Impact of cyberattack(s)

Data loss emerged as the most frequently reported impact, with 70 respondents (26.5%) indicating that their systems experienced a loss of data. Data loss can have severe consequences, including compromised privacy, potential legal ramifications, and disruption of regular operations. Stolen personal information was reported by 67 (25.4%) respondents, highlighting the alarming extent to which cyberattacks can lead to the unauthorised acquisition of sensitive personal data. Such breaches can result in identity theft, financial fraud, and long-term personal security risks. A significant number of 55 respondents (20.8%) reported the disruption of services as an impact of cyberattacks. Service disruptions can lead to operational downtime, affecting productivity and potentially causing financial losses. Financial loss was identified by 39 respondents (14.8%), indicating the monetary implications resulting from cyberattacks. Financial losses may include direct costs related to recovery efforts, as well as indirect costs stemming from reputational damage and customer trust erosion. Reputation damage was cited by 31 respondents (11.7%) as a consequential impact of cyberattacks. A tarnished reputation can have enduring effects on an individual's or organization's credibility, potentially impacting trust among stakeholders.

4.6.1.5. In your opinion, what are the most significant cybersecurity challenges faced by rural communities in Mopani District?

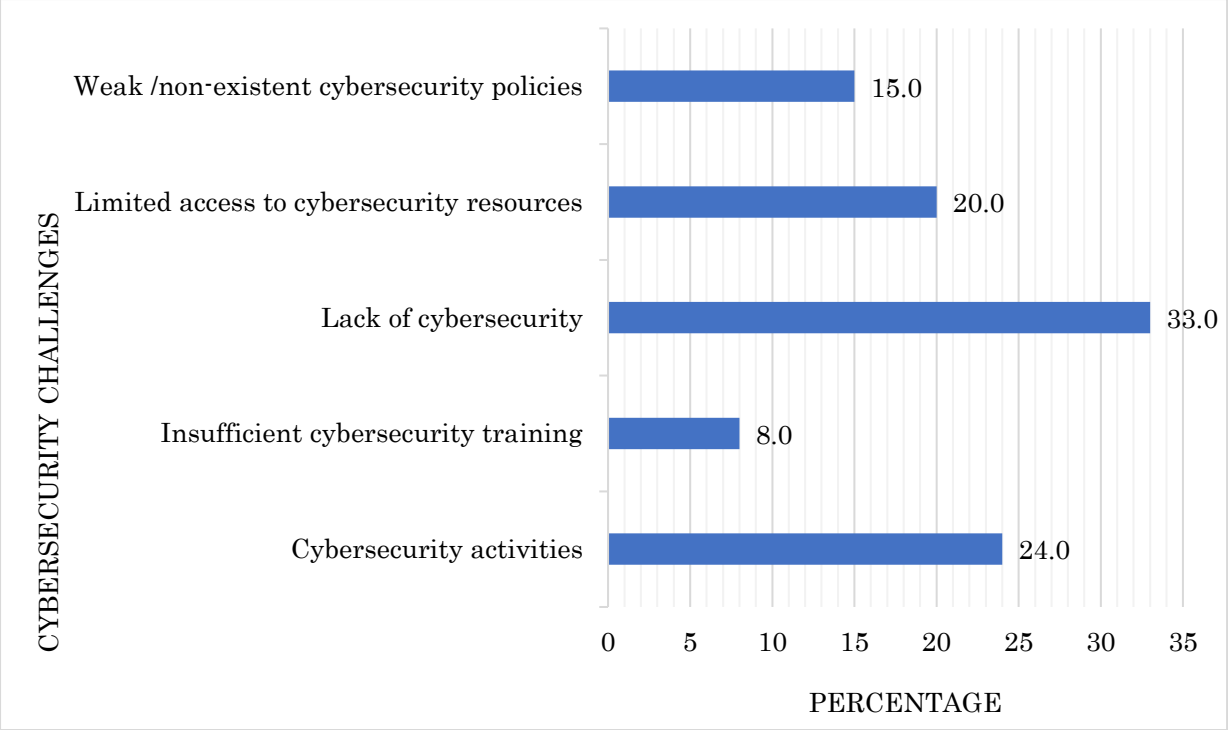

Figure 4.10: Cybersecurity challenges faced by rural communities of Mopani District

The analysis in Figure 4.10 illustrates the cybersecurity challenges confronted by rural communities in the Mopani District. Among these challenges, the lack of cybersecurity emerged as the most significant, garnering 33% of responses. Cybersecurity activities were also identified as a substantial challenge, accounting for 24% of responses. Limited access to cybersecurity resources was reported by 20% of respondents as a noteworthy challenge. Additionally, weak or non-existent cybersecurity policies were highlighted by 15% of respondents, and insufficient cybersecurity training was identified by 8% of the respondents. These challenges collectively contribute to the facilitation or prevalence of cyberattacks within the district.

4.7. SECTION C: FACTORS INFLUENCING CYBERSECURITY POLICIES

In this section, the focus shifted to the critical factors that shape the landscape of cybersecurity policies within the Mopani District. The exploration begins by delving into the awareness of respondents regarding existing local cybersecurity policies or initiatives. Participants were encouraged to express their familiarity with these policies, and if so, to specify the particular policies or initiatives they are cognizant of. Moving forward, the researcher embarked on unraveling the complex network of influences that contribute to the development and implementation of cybersecurity policies in rural communities like Mopani. Respondents were invited to share insights into the factors they perceive as significant in this context. The options provided encompass a broad spectrum of potential influences, ranging from government support and regulations to community engagement and awareness, the availability of cybersecurity expertise, funding and resources, and collaboration with local organizations.

This comprehensive exploration aimed to capture the nuanced interplay of factors that shape the cybersecurity policy landscape in the Mopani District. By understanding the perceptions and priorities of respondents, the researcher aimed to discern the key drivers and challenges that influence the formulation and execution of cybersecurity policies within rural communities. This information serves as a foundational resource for developing targeted strategies and interventions to enhance cybersecurity resilience in the Mopani District.

4.7.1. Are you aware of any local cybersecurity policies or initiatives in the Mopani District?

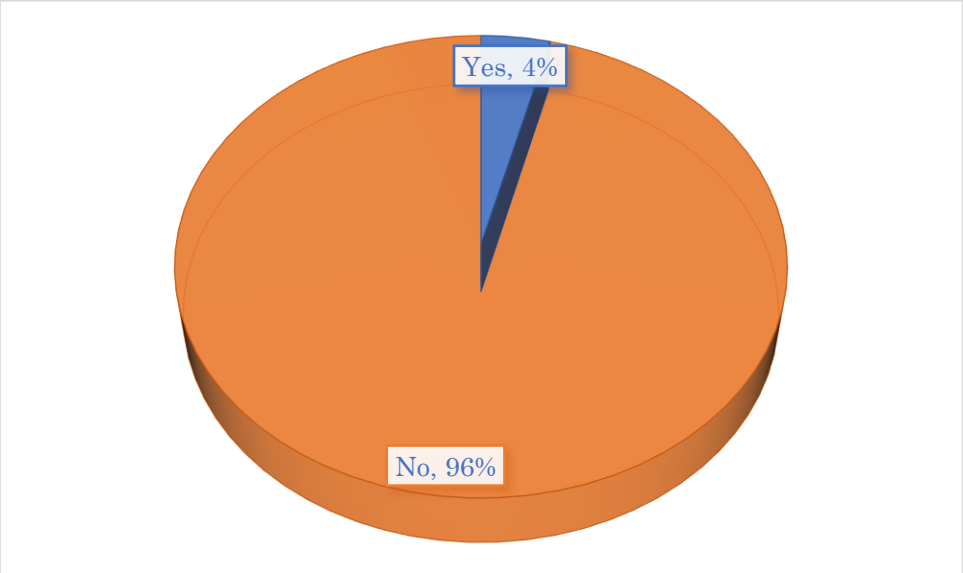

Figure 4.11: Awareness of local cybersecurity policies

The findings portrayed in Figure 4.11 reveal a substantial lack of awareness among the respondents regarding local cybersecurity policies or initiatives. A staggering 96% of the respondents indicated that they are unaware of any such policies or initiatives, while a mere 4% expressed awareness. These results point to a significant gap in knowledge and awareness regarding cybersecurity-related measures in the Mopani District. The overwhelming lack of awareness suggests that there may be a dearth of robust campaigns or accessible information regarding various aspects of cybersecurity within the Mopani District. It implies that the community is not well-informed about the existence, content, or significance of local cybersecurity policies or initiatives. Furthermore, these findings raise the possibility that there might be limited, if any, cybersecurity measures in place within the Mopani District, contributing to the prevailing lack of awareness among the respondents.

In essence, the low level of awareness underscores the need for increased efforts in disseminating information, fostering campaigns, and potentially developing and implementing cybersecurity policies in the region. Addressing this informational gap is crucial to enhancing the overall cybersecurity posture of the Mopani District and empowering its residents to navigate the digital landscape with greater awareness and resilience.

4.7.2. If yes, can you please select the cybersecurity policies or initiatives you are aware of in the Mopani District?

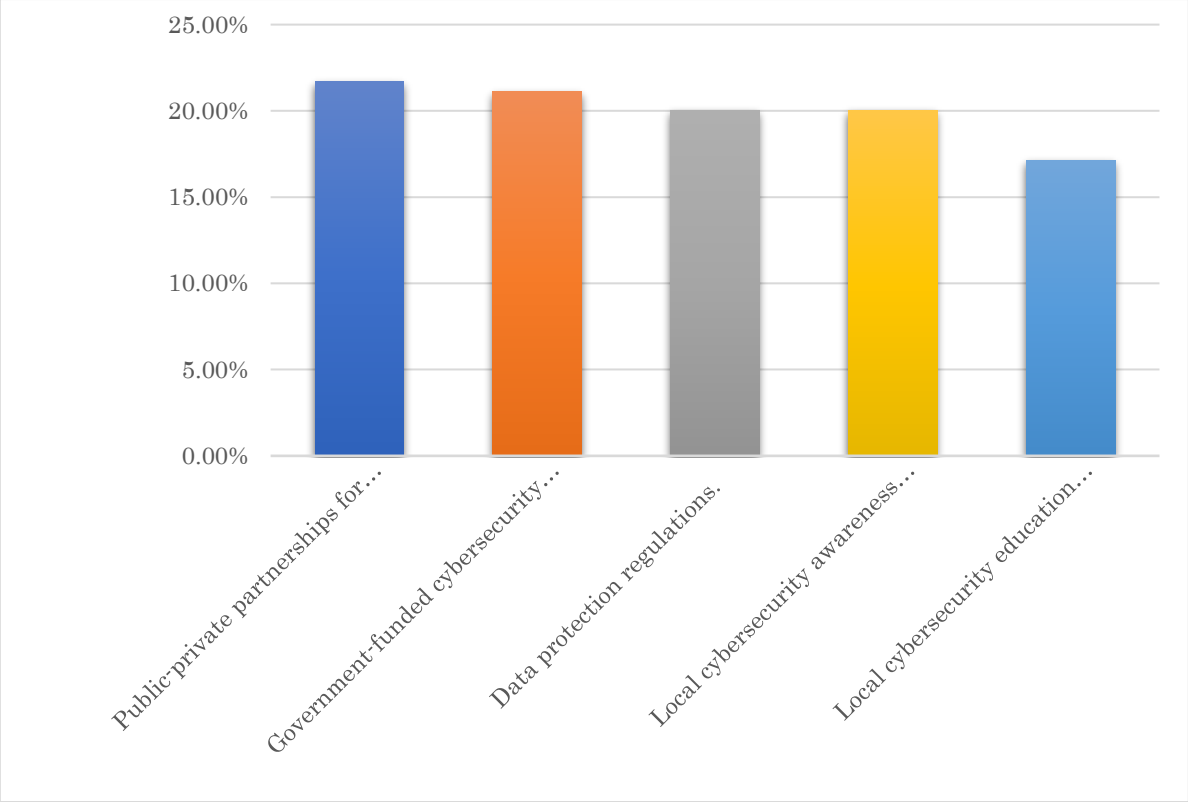

Figure 4.12: Local cybersecurity policies in the Mopani district

Public-private partnerships for cybersecurity emerged as the most prominently recognised initiative, with 38 respondents (21.7%) expressing awareness of such collaborations. These partnerships are pivotal in fostering collaborative efforts between government entities and private organizations, contributing significantly to enhancing the overall resilience of cybersecurity measures. The acknowledgment of government-funded cybersecurity programs by 37 respondents (21.10%) underscores the importance of state-sponsored initiatives in fortifying cybersecurity measures. Such programs typically involve financial support for cybersecurity initiatives, comprehensive training, and the development of critical cybersecurity infrastructure.

Furthermore, respondents recognised the significance of data protection regulations, with 35 individuals (20%) indicating awareness of such policies. These regulations play a vital role in safeguarding individuals' privacy and ensuring responsible handling of sensitive information. The acknowledgment of local cybersecurity awareness campaigns by 35 respondents (20.0%) highlights the crucial role of grassroots efforts in educating the community on cybersecurity matters. These campaigns contribute significantly to building a cyber-resilient community by empowering individuals with knowledge and best practices. Thirty respondents expressed awareness of local cybersecurity education initiatives, underscoring the importance of educational programs in equipping individuals with the necessary knowledge and skills in

cybersecurity. These education initiatives aim to bridge the knowledge gap and empower individuals to navigate the digital landscape securely. Overall, these findings emphasise the multifaceted approach required to bolster cybersecurity awareness and resilience, involving collaborative partnerships, government-sponsored programs, regulatory frameworks, and grassroots educational efforts.

4.7.3. What factors do you believe influence the development and implementation of cybersecurity policies in rural communities like Mopani?

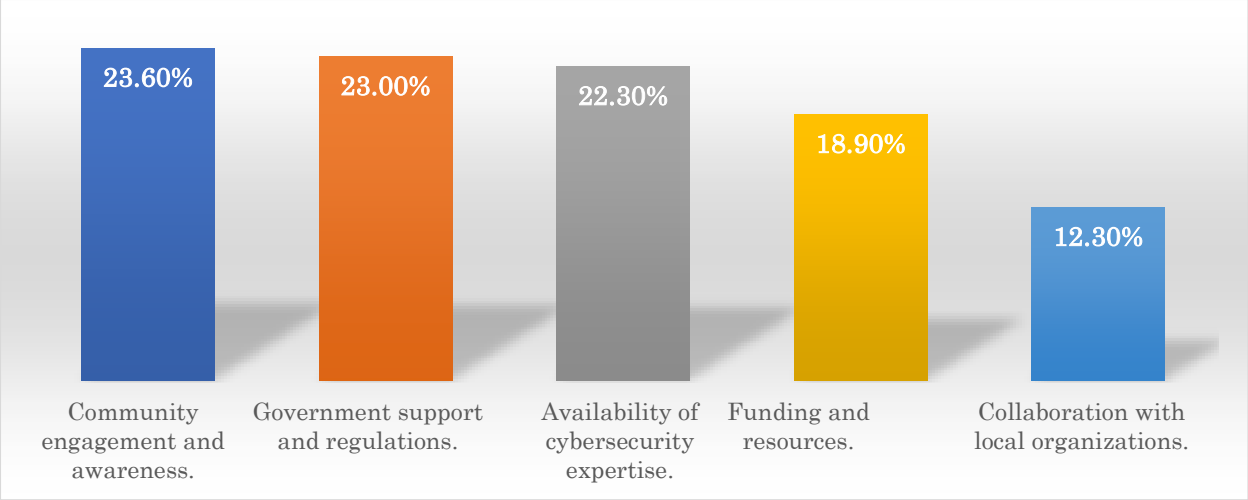

Figure 4.13: Factors that influence the development and implementation of cybersecurity policies

From the figure 4.13, the majority of respondents, comprising 153 individuals (23.6%), underscored the critical role of community engagement and awareness in shaping effective cybersecurity policies. This highlights the significance of actively involving local communities in cybersecurity initiatives and conducting awareness campaigns to enhance understanding and cooperation. The emphasis on community engagement aligns with the notion that building a cyber-resilient environment necessitates the active participation and awareness of the people it seeks to protect. Government support and regulatory frameworks emerged as pivotal factors influencing cybersecurity policy development, as recognised by 149 respondents (23%). Advocacy for government involvement and the establishment of clear regulations to guide cybersecurity practices in rural areas are pivotal considerations. This signifies the importance of a regulatory framework to provide guidance and structure to cybersecurity efforts, especially in rural settings.

Furthermore, 144 respondents (22.3%) highlighted the significance of having access to cybersecurity expertise in rural communities. Addressing this challenge involves the implementation of initiatives such as training programs, knowledge-sharing platforms, and partnerships with cybersecurity professionals. Enhancing expertise within rural communities

contributes to building a knowledgeable and skilled populace capable of navigating the evolving cybersecurity landscape. The availability of funding and resources emerged as a critical factor, with 122 respondents (18.9%) recognising its impact on the development and implementation of cybersecurity policies. Identifying sustainable funding sources and optimising resource allocation are essential components in overcoming this challenge. Adequate financial support is crucial for executing effective cybersecurity strategies and sustaining long-term initiatives.

Lastly, collaboration with local organizations was identified by 78 respondents (12.3%) as a contributing factor in cybersecurity policy development. Building partnerships with local entities can foster a collaborative approach to addressing cybersecurity challenges and leverage shared resources. This collaborative spirit enhances the overall resilience of rural communities against cybersecurity threats and fosters a collective response to the evolving landscape of digital security.

4.8. SECTION D: CYBERSECURITY AWARENESS

This section focuses on cybersecurity awareness, aiming to assess the knowledge and proactive engagement of respondents in the Mopani District. The participants were prompted to rate their awareness of cybersecurity concepts, offering valuable insights into the level of familiarity with essential cybersecurity principles. This initial assessment provides a foundational understanding of the participants' baseline knowledge in the realm of cybersecurity. To gain deeper insights into the habits and behaviours of respondents, the inquiry extends to the frequency with which individuals actively seek information about cybersecurity threats and best practices. Responses were categorised into daily, weekly, monthly, rarely, or never, allowing for the analysis of patterns in information-seeking behavior within the community. This segmentation helped in understanding the regularity and intensity of the community's engagement with cybersecurity-related information.

Furthermore, the section delves into the extent of cybersecurity training or education received, specifically tailored to rural communities in Mopani. Participants were prompted to specify the type of training they have undergone, encompassing a spectrum from workshops and online courses to in-person sessions and educational materials. This detailed exploration enabled a nuanced understanding of the diverse educational avenues available and preferred within the community. Additionally, respondents who have received training were invited to evaluate its effectiveness, offering valuable feedback on the impact of cybersecurity education within the local context. This evaluative component was crucial in assessing the practical utility and perceived value of the cybersecurity training initiatives undertaken in the Mopani District. These inquiries contribute to a comprehensive analysis of the cybersecurity awareness landscape within the community, informing future strategies and interventions tailored to the specific needs and preferences of the respondents.

4.8.1. What is the level of cybersecurity awareness among rural communities in the Mopani District of Limpopo Province?

To implement relevant cybersecurity awareness; the respondents were asked as to whether they were aware of cybersecurity. Several questions were asked to deduce the level of understanding the respondents have about cybersecurity. The questions asked involved:

Table 4.2: Cybersecurity Awareness

Variable	Category	Frequency	Percent

How would you rate your awareness of cybersecurity concepts?	Not Aware	121	60.5%
	Very Aware	35	17.5%
	Extremely Aware	21	10.5%
	Moderately Aware	15	7.5%
	Slightly Aware	8	4.0%
How often do you actively seek information about cybersecurity threats and best practices?	Never	117	58.50%
	Rarely	39	19.50%
	Daily	27	13.50%
	Monthly	11	5.50%
	Weekly	6	3.00%
If received any, how effective did you find the cybersecurity training or education you received in rural communities in Mopani?	Very Effective.	27	13.50%
	Somewhat Effective.	12	6.00%
	Not Very Effective.	108	54.00%
	Not Effective at All.	9	4.50%

In the surveyed population of the Mopani District, the awareness of cybersecurity concepts varied among respondents. A significant proportion reported being Not Aware (60.5%), while 17.5% considered themselves Very Aware, and 10.5% described their awareness as Extremely Aware. Moderately aware and slightly aware categories accounted for 7.5% and 4.0%, respectively. Regarding information-seeking habits about cybersecurity, the majority of respondents indicated infrequent engagement. A notable 58.50% reported Never actively seeking information, followed by Rarely at 19.50%. A smaller percentage engaged more regularly, with 13.50% choosing Daily, 5.50% Monthly, and 3.00% Weekly. In terms of the effectiveness of cybersecurity training or education received in rural communities in Mopani, respondents provided diverse perspectives. The largest group, constituting 54.00%, found the training Not Very Effective, while 13.50% considered it Very Effective.

4.8.2. Type of cybersecurity training or education received specific to rural communities in Mopani:

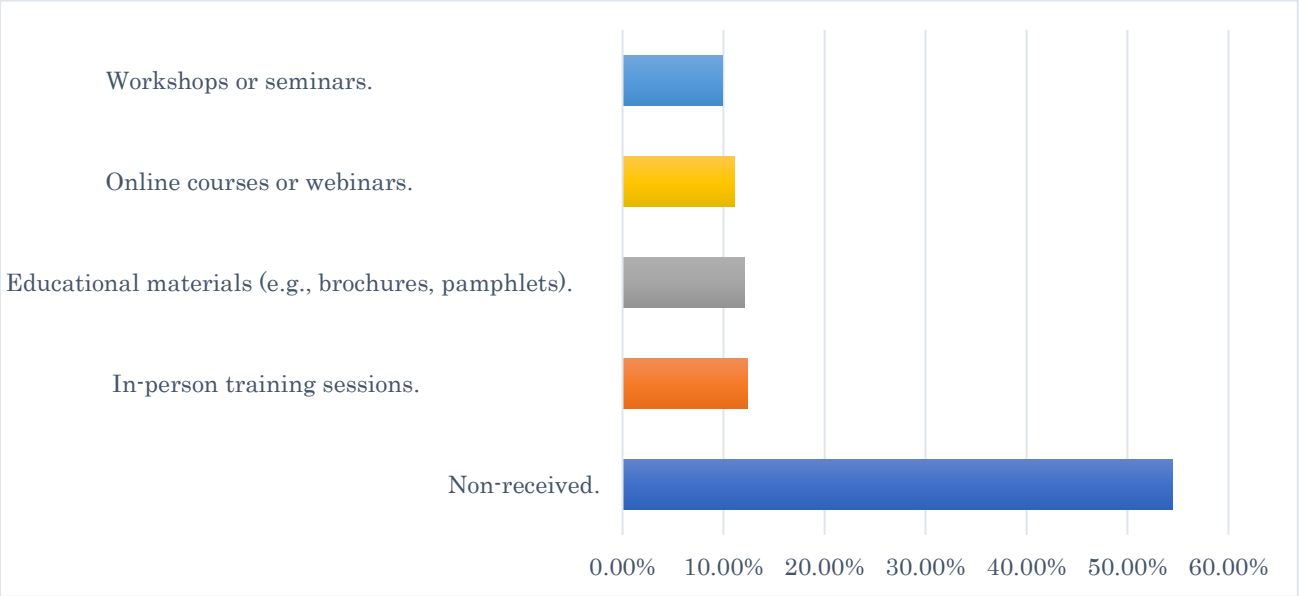

Figure 4.14: Type of cybersecurity training or education received specific to rural communities in Mopani

A notable portion of respondents, comprising 176 (54.5%), revealed that they have not received any specific cybersecurity training or education tailored to rural communities in the Mopani District. This highlights a significant opportunity to explore and implement targeted training initiatives aimed at addressing the current gap in cybersecurity education within the community. Among the respondents who received cybersecurity education, in-person training sessions were recognised by 40 (12.4%). This mode of cybersecurity education offers the advantage of direct interaction, allowing participants to engage with trainers, ask questions, and participate in hands-on activities. The interactive nature of in-person sessions enhances the learning experience and facilitates a more comprehensive understanding of cybersecurity principles. Educational materials, such as brochures and pamphlets, were acknowledged by 39 (12.1%) respondents as a valuable source of cybersecurity information. Providing written materials serves as a supplementary method to disseminate essential cybersecurity concepts and best practices, catering to diverse learning preferences. Online courses or webinars were cited by 36 (11.1%) respondents, indicating a preference for digital learning platforms in cybersecurity education. Online courses offer flexibility, allowing participants to access training materials at their own pace and convenience, making cybersecurity education more accessible. Workshops or seminars were identified by 32 (9.9%) respondents as a form of cybersecurity training. Workshops and seminars provide opportunities for interactive learning,

group discussions, and the practical application of cybersecurity principles, fostering a dynamic and engaging educational environment. Therefore, these findings underscore the varied preferences and opportunities for delivering cybersecurity education, suggesting the need for a multifaceted approach to address the diverse learning needs within the Mopani District.

4.9. SECTION E: RURAL COMMUNITIES' ATTITUDE TOWARDS CYBERSECURITY.

In this section, the researcher delved into the attitudes and perceptions of individuals within the Mopani District regarding cybersecurity in rural communities. Respondents were asked to express their level of agreement with a series of statements that touch upon the importance of cybersecurity for community safety, concerns about potential threats, the belief in the necessity of cybersecurity education, and the consideration of investing in cybersecurity measures and tools. Each statement provides a spectrum of responses, ranging from "Strongly Agree" to "Strongly Disagree," allowing participants to articulate their individual perspectives. By gathering these insights, the researcher aimed to paint a nuanced picture of the community's collective attitude towards cybersecurity, identifying areas of consensus or divergence in opinions. Additionally, participants were asked to rate the overall level of awareness about cybersecurity among residents in the rural community, providing a holistic view of the community's self-perception regarding its preparedness and understanding of cybersecurity issues.

4.9.1. What is the attitude of rural communities towards cybersecurity?

- The attitude of rural communities of the Mopani district towards cybersecurity was assessed.
- The Likert scale assessment aided in understanding these attitudes by the rural communities in the district.

Table 4.3: Rural Communities' Attitude towards cybersecurity

Statement	S.agree	Agree	Neutral	Disagree	S.disagree	Mean	SD
Cybersecurity is important for the safety of our community	(49) 24.50%	(0) 0.00%	(4) 2.00%	(28) 14.00%	(119) 59.50%	3.8	1.676
I am concerned about the potential cybersecurity threats that affect our community	(64) 32.00%	(1) 0.50%	(5) 2.50%	(24) 12.00%	(106) 53.00%	3.54	1.801
I believe that individuals in our community should be educated about cybersecurity.	(66) 33.00%	(1) 0.50%	(3) 1.50%	(20) 10.00%	(110) 55.00%	3.54	1.832
Our community should invest in cybersecurity measures and tools	(66) 33.00%	(0) 0.00%	(5) 2.50%	(24) 12.00%	(105) 52.50%	3.51	1.816

In the examined Mopani District population, perceptions regarding the importance of cybersecurity displayed notable diversity. A considerable proportion expressed a strong stance, with 24.50% strongly agreeing that cybersecurity is crucial for community safety. In contrast, a mere 2.00% affirmed agreement, while 14.00% maintained a neutral standpoint. Conversely, a substantial 59.50% disagreed, signaling a varying range of perspectives within the community. The mean score of 3.8, with a standard deviation of 1.676, further emphasises the dispersion and central tendency of attitudes. Regarding concerns about potential cybersecurity threats, 32.00% strongly agreed, underscoring a heightened level of apprehension. In contrast, only 0.50% expressed agreement, while 2.50% maintained a neutral position. The disagreement spectrum encompassed 12.00%, and a significant 53.00% strongly disagreed. The mean score of 3.54, with a standard deviation of 1.801, illustrates the

varying degrees of concern within the community. Furthermore, the belief that individuals in the community should be educated about cybersecurity revealed a pronounced sentiment. A substantial 33.00% strongly agreed, while only 0.50% indicated agreement. The neutral stance was expressed by 1.50%, and 10.00% disagreed, while a noteworthy 55.00% strongly disagreed. The mean score of 3.54, with a standard deviation of 1.832, highlights the dispersion and central tendency of views on the necessity of cybersecurity education. In terms of community investment in cybersecurity measures and tools, a significant 33.00% strongly agreed, reflecting a proactive stance. Neutral perspectives were expressed by 2.50%, while 12.00% disagreed, and 52.50% strongly disagreed. The mean score of 3.51, with a standard deviation of 1.816, elucidates the community's varying degrees of willingness to invest in cybersecurity.

4.9.2. How would you rate the level of awareness about cybersecurity among residents in our rural community?

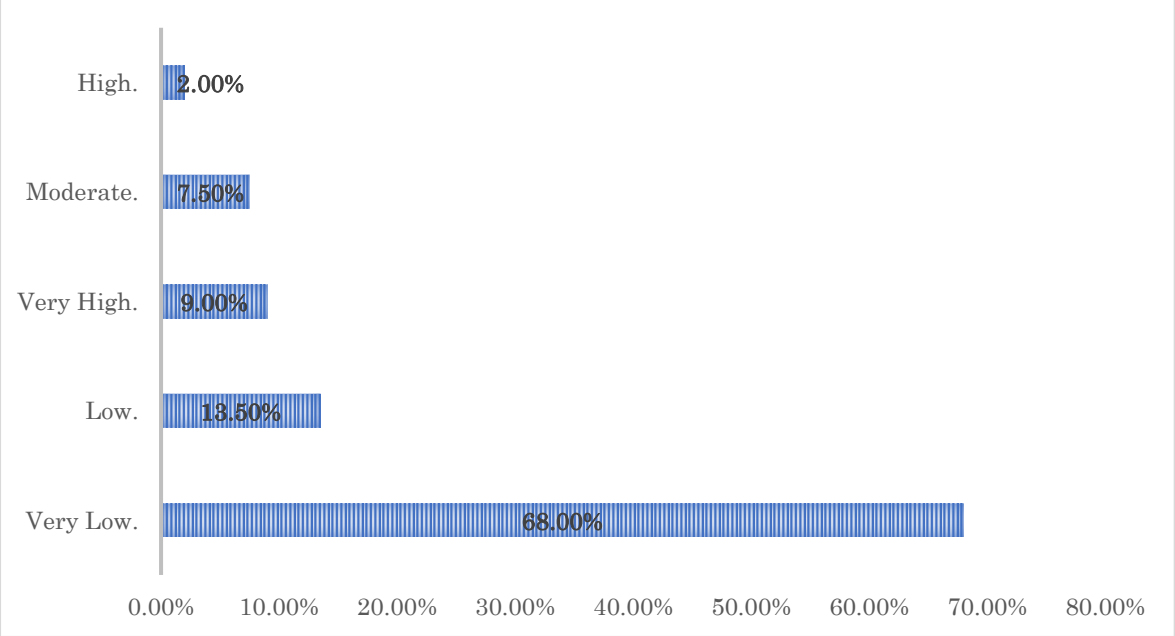

Figure 4.15: Level of cybersecurity awareness

The findings depicted in Figure 4.15 shed light on the respondents' perceptions regarding the level of awareness about cybersecurity among residents in their rural community. A significant majority, constituting 68% of the respondents, expressed a prevailing belief that the awareness about cybersecurity within the community is rated as very low. This substantial percentage underscores a critical need for comprehensive and targeted community-wide awareness campaigns. The notable prevalence of a very low awareness rating suggests that there is a considerable gap in understanding and knowledge about cybersecurity practices and threats within the rural community. Such a gap may potentially expose community

members to various cyber risks due to a lack of awareness and knowledge. Furthermore, 9% rated Very High, 7.50% Moderate, 13.50% Very low, and contrastingly, only a minimal 2% of the respondents reported a high level of awareness about cybersecurity among residents. This minority acknowledgment of a high awareness level indicates that there may be a small segment of the community actively engaged and informed about cybersecurity practices.

4.10. SECTION F: CYBERSECURITY STRATEGIES (CONSTRUCT).

In this section, the researcher shifted the focus to the cybersecurity strategies implemented by individuals within the Mopani District. This section was meticulously crafted to delve into the practices and habits embraced by the respondents in safeguarding their digital presence. Through a series of targeted questions, the aim was to assess and understand the sources relied upon for cybersecurity information, the robustness of password practices, the regularity of software and application updates, and the level of caution exercised when dealing with emails from unfamiliar senders. Participants were invited to articulate the channels from which they derive cybersecurity information, including the internet, workshops/training sessions, social media, and advice from friends or family. This exploration into information sources provided crucial insights into the community's diverse reliance on various channels to stay well-informed about the best practices in cybersecurity.

Furthermore, this section delves into the personal cybersecurity habits of respondents, encompassing key aspects such as the adoption of strong, unique passwords, the frequency of software and application updates, and the prudence exercised when encountering links or attachments in emails from unknown senders. By garnering responses to these pertinent questions, the goal was to uncover prevailing cybersecurity practices within the community and identify areas that may benefit from heightened awareness or targeted educational initiatives.

4.10.1. Cybersecurity Strategies and Awareness.

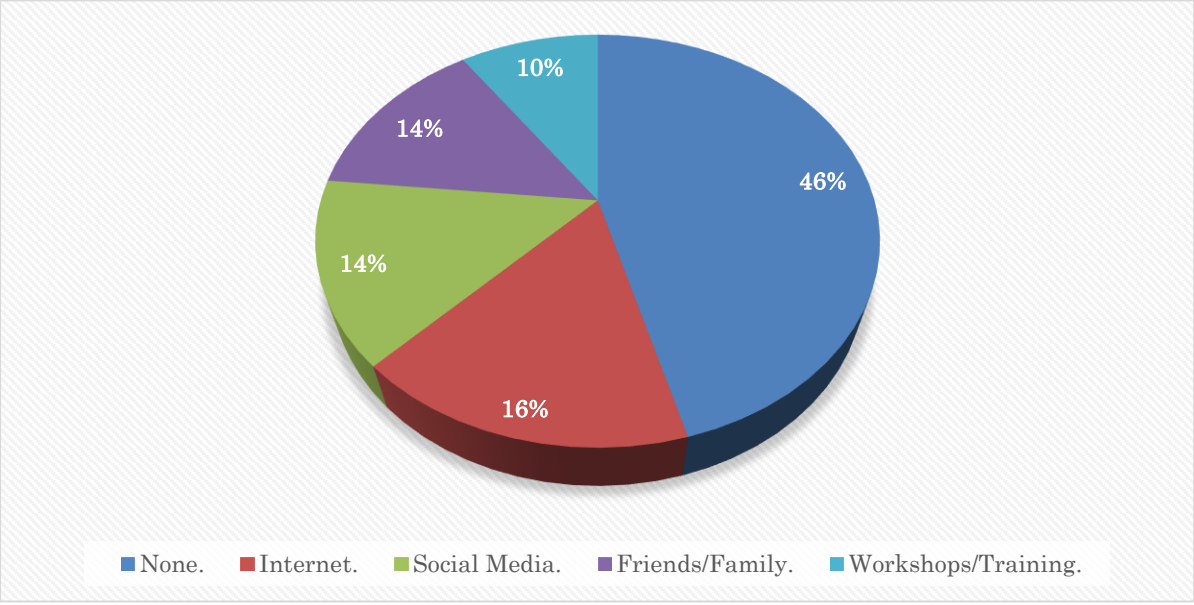

Figure 4.16: Types of sources for cybersecurity information

A significant portion of respondents, comprising 153 individuals (45.8%), indicated that they do not depend on any specific source for cybersecurity information. This notable finding highlights the imperative to develop strategies that effectively reach and educate individuals who currently lack dedicated sources for cybersecurity information. Among those who identified specific sources, 55 respondents (16%) recognised the internet as a significant channel for obtaining cybersecurity information. The internet, with its expansive repository of resources including articles, blogs, official documentation, and expert insights, stands out as a comprehensive platform for accessing diverse cybersecurity knowledge. Social media platforms were acknowledged by 48 respondents (14.4%) as notable sources of cybersecurity information. These platforms offer a dynamic space for sharing cybersecurity tips, news, and engaging in discussions, thereby contributing to community-wide awareness. Friends and family emerged as influential sources for cybersecurity information, as noted by 46 respondents (13.8%). Informal networks play a crucial role in sharing practical experiences, insights, and advice related to cybersecurity practices.

Workshops and training sessions were identified by 32 respondents (9.60%) as valuable sources of cybersecurity information. These formal training programmes and workshops provide structured learning opportunities, empowering individuals with practical cybersecurity knowledge and skills. This multifaceted exploration of information sources offers valuable insights into the varied channels through which individuals in the community seek and receive cybersecurity information.

Table 4.4: Cybersecurity Strategies

Variable	Category	Frequency	Percentage
Do you use strong, unique passwords for your online accounts?	Rarely.	133	66.50%
	Always.	41	20.50%
	Often.	21	10.50%
	Never.	5	2.50%
How frequently do you update your software and applications to the latest versions?	Never.	114	57.00%
	Rarely.	38	19.00%
	Always.	36	18.00%
	Often.	12	6.00%
Are you cautious about clicking on links or attachments in emails from unknown senders?	Rarely.	149	74.50%
	Always.	34	17.00%
	Never.	9	4.50%
	Often.	8	4.00%

Table 4.4 reveals that 66.5% of respondents rarely use strong, unique passwords, highlighting a critical vulnerability in password practices. To address this issue in the Mopani District, practical steps could include conducting community workshops on the importance of strong passwords and implementing password management tools. Educational campaigns should focus on demonstrating how to create and manage strong, unique passwords and the benefits of multi-factor authentication. Additionally, 57% of respondents reported that they either never or rarely update their software and applications, indicating a need for targeted educational efforts on the importance of timely updates. Practical measures could involve organising local seminars or online tutorials on software updates, providing step-by-step guides, and potentially offering support through community tech hubs to help residents keep their systems current with the latest security patches. The finding that 74.5% of respondents rarely exercise caution when clicking on links or attachments from unknown senders underscores the need for anti-phishing training. Implementing community-wide initiatives that focus on recognising and avoiding phishing attempts can enhance cybersecurity awareness. These could include

interactive workshops, distribution of educational materials, and simulated phishing exercises to build a culture of vigilance and improve the community's overall cybersecurity posture.

4.11. SECTION G: CYBERSECURITY TOOLS (CONSTRUCT).

In this section, the researcher investigated the utilization of cybersecurity tools within the Mopani District, aiming to assess the awareness, accessibility, and adoption of essential security measures by community members. This section comprehensively explored various aspects, ranging from personal device protection to community-wide cybersecurity strategies. To begin, participants were asked about their use of antivirus or anti-malware software on their devices, providing valuable insights into individual-level security practices. Additionally, respondents were prompted to specify the type of firewall protection employed on their home networks, allowing us to distinguish between hardware and software firewalls. The survey further delved into the awareness of encryption practices to secure data on personal devices and the accessibility of cybersecurity tools within the community. Participants were asked whether they are familiar with particular cybersecurity strategies or tools implemented in the Mopani District, enabling the researcher to gauge the extent of knowledge about local initiatives.

In cases where respondents express awareness of community-level cybersecurity tools, the survey assessed their perceived accessibility. By categorising responses as "Very Accessible," "Somewhat Accessible," or "Not Accessible," the objective was to understand the ease with which community members can leverage these tools for enhanced online security. This multifaceted approach allowed a comprehensive investigation of the cybersecurity landscape within the Mopani District, providing insights into both individual and community-level security practices.

4.11.1. Cybersecurity Tools Used

Table 4.5: Cybersecurity Tools

Statement(s)	Category	Frequency	Percentage
Do you use any antivirus or anti-malware software on your devices?	No	166	83.00%
	Yes	34	17.00%
What type of firewall protection do you have on your home network?	No Firewall	184	92.00%
	Software Firewall	11	5.50%
	Hardware	5	2.50%
Are you aware of the use of encryption to secure data on your devices?	No	156	78.00%
	Yes	44	22.00%
Is there access to cybersecurity tools (e.g., antivirus software) within your community?	No	162	81.00%
	Yes	38	19.00%
Are you aware of any cybersecurity strategies or tools used in the Mopani District to enhance online security?	No	161	80.50%
	Yes	39	19.50%
If any you are aware of any cybersecurity strategies, how accessible are these tools to community members?	Very Accessible.	26	13.00%
	Not Accessible.	13	6.50%
	Somewhat Accessible.	12	6.00%

The findings reveal that a significant majority of respondents (83%) do not utilise antivirus or anti-malware software, underscoring the imperative for community-wide adoption of fundamental cybersecurity tools. Initiatives aimed at encouraging the use of these foundational tools can substantially enhance digital security within the community. Furthermore, a notable percentage (92%) of respondents lack any firewall protection on their home network. Promoting the adoption of both software and hardware firewall protection becomes crucial in mitigating potential security risks and fortifying overall network security. The survey also brings to light that (78%) of respondents are not aware of the use of encryption

to secure data on their devices. This emphasises the need for educational efforts on encryption and its benefits to reinforce data security practices within the community. Moreover, a substantial portion (81%) of respondents lack awareness of the availability of cybersecurity tools within their community. Tailored strategies should be implemented to enhance the accessibility of these tools, fostering a safer digital environment for community members.

In addition, a significant number of respondents (80.5%) are not aware of any cybersecurity strategies or tools employed in the Mopani District. This underscores the necessity for comprehensive awareness campaigns to inform residents about existing cybersecurity initiatives, contributing to a more informed and secure community. Interestingly, only a small percentage (13%) perceives cybersecurity tools as very accessible, while (6.5%) find them not accessible at all. This highlights the need for concerted efforts to improve accessibility, ensuring that community members can readily access and benefit from available cybersecurity tools.

4.11.2. Cybersecurity strategies or tools awareness in the Mopani District

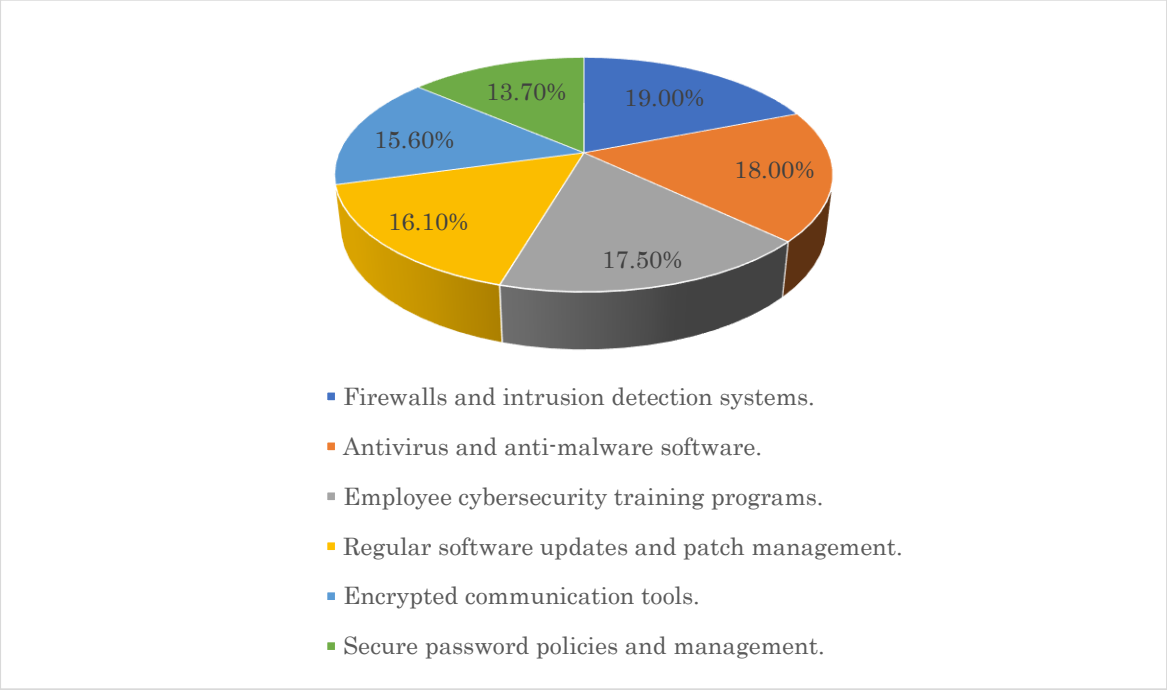

Figure 4.17: Cybersecurity strategies or tools awareness in the Mopani District

In the Mopani District, the rates of adoption for various cybersecurity strategies are as follows: firewalls and intrusion detection systems (19.0%), antivirus and anti-malware software (18.0%), employee cybersecurity training programs (17.5%), regular software updates and patch management (16.1%), encrypted communication tools (15.6%), and secure password policies and management (13.7%). These figures offer insights into the prevalence of specific

cybersecurity measures within the community, providing a snapshot of the current state of cybersecurity practices in the Mopani District. They serve as a guide for identifying potential areas of focus in future initiatives aimed at strengthening overall cybersecurity resilience.

4.12. SECTION H: DETERRENCE (CONSTRUCT).

This section delves into the concept of deterrence in cybersecurity within rural communities, with a specific focus on the Mopani District. The primary objective of this section was to assess respondents' opinions regarding the effectiveness of implementing cybersecurity measures as a deterrent against cybercriminal activities. Participants were encouraged to articulate their perspectives by choosing from a spectrum of responses, ranging from "Strongly Agree" to "Strongly Disagree." This nuanced approach allowed researcher to glean valuable insights into the perceived impact of cybersecurity measures in deterring cybercriminals within the community. Furthermore, the survey explored respondents' views on additional cybersecurity measures that could potentially serve as effective deterrents. The provided options encompass a diverse array of strategies, including the improvement of cybersecurity education and awareness programs, the reinforcement of local law enforcement's capacity to address cybercrime, the promotion of stronger cybersecurity practices in businesses, the advocacy for multi-factor authentication (MFA), the enhancement of local cybersecurity infrastructure, the implementation of stricter penalties for cybercriminals, and the fostering of collaboration between local organizations and government agencies.

By collecting opinions on these proposed measures, the aim was to discern the community's preferences and priorities concerning cybersecurity deterrence strategies. This invaluable information played a pivotal role in shaping recommendations and initiatives aimed at fortifying the cybersecurity resilience of the Mopani District, ultimately fostering a safer online environment for its residents.

Table 4.6: Deterrence

Variable	Category	Frequency	Percentage
Do you believe that implementing effective cybersecurity measures can deter cybercriminals in rural communities like Mopani?	Strongly Agree.	52	26.00%
	Agree.	0	0
	Neutral.	7	3.50%
	Disagree.	28	14.00%
	Strongly Disagree	113	56.50%

Upon scrutinising the community's perspectives on the effectiveness of implementing cybersecurity measures to deter cybercriminals in rural areas, particularly in Mopani, the following frequencies and percentages were discerned: 26.00% strongly agreed (n = 52), 0.00% agreed (n = 0), 3.50% were neutral (n = 7), 14.00% disagreed (n = 28), and 56.50% strongly disagreed (n = 113). These findings unveil a significant disparity in opinions within the community. A noteworthy portion of respondents strongly affirms the efficacy of cybersecurity measures in deterring cybercriminals, constituting a considerable segment of the community. In contrast, a substantial majority firmly expresses strong disagreement with the notion. The conspicuous absence of responses in the "Agree" category implies a polarised perspective on the perceived impact of cybersecurity measures in rural settings like Mopani. These nuanced results contribute to a comprehensive understanding of the community's beliefs regarding the role of cybersecurity in deterring cybercrime.

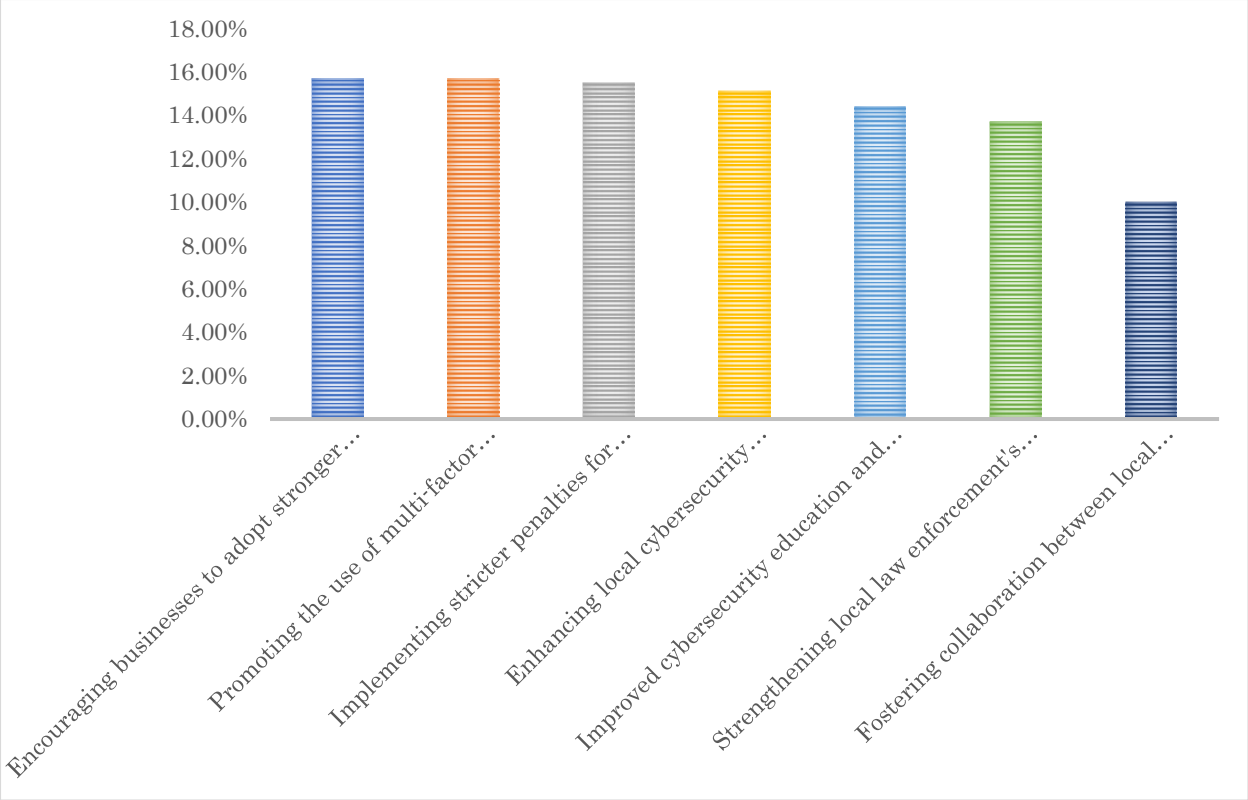

Figure 4.18: Cybersecurity measures that can serve as a deterrent to cybercriminal activities

Within the Mopani district, diverse perspectives emerge regarding the adoption of strategies aimed at enhancing cybersecurity. The adoption rates for various cybersecurity enhancement strategies are as follows: Encouraging businesses to adopt stronger cybersecurity practices stands out with an adoption rate of 15.7%, reflecting significant community support for initiatives promoting robust cybersecurity measures within local businesses. Similarly, the promotion of multi-factor authentication (MFA) also garners an adoption rate of 15.7%, indicating a community inclination towards embracing advanced authentication methods to bolster online security. A noteworthy 15.5% of the community supports the implementation of stricter penalties for cybercriminals, highlighting a shared belief in the importance of robust legal measures to deter and punish cybercrime. The enhancement of local cybersecurity infrastructure receives support from 15.1% of the community, indicating a recognition of the crucial role that infrastructure plays in safeguarding digital environments. Improved cybersecurity education and awareness programmes garner a significant adoption rate of 14.4%, underlining the community's commitment to fostering knowledge and awareness regarding cyber threats. Strengthening local law enforcement's capacity to address cybercrime is endorsed by 13.7% of the community, suggesting a desire for enhanced law enforcement capabilities in tackling cyber threats. Fostering collaboration between local

organizations and government agencies, while slightly lower at 10.0%, still reflects a degree of community interest in cooperative efforts to address cybersecurity challenges.

4.13. Correlation and Regression Analysis

According to Brink et al. (2018), correlation elucidates the relationships among different variables within a dataset. Correlation coefficients range from -1 to 1, with 1 indicating a strong positive correlation, -1 indicating a strong negative correlation, and 0 indicating no correlation. Regression, on the other hand, is a statistical method that explores the relationship between a dependent variable and one or more independent variables (Brink et al., 2018). In this study, regression and correlation analyses were employed to discern the relationships and significance between the independent variable (cybersecurity awareness strategy) and dependent variables (cybersecurity challenges, factors, awareness, strategies, tools, and deterrence). Below presents the correlation and regression analysis:

Given the context, the formulas for regression and correlation are:

4.13.1. Correlation Coefficient (Pearson's r) Equation:

$$r = \frac{N(\sum XY) - (\sum X)(\sum Y)}{\sqrt{[N\sum X^2 - (\sum X)^2][N\sum Y^2 - (\sum Y)^2]}}$$

Figure 4.19: Correlation Coefficient Equation

Where:

N is the number of pairs of scores

$\sum XY$ is the sum of the products of paired scores

$\sum X$ and $\sum Y$ are the sums of the X scores and Y scores respectively

$\sum X^2$ and $\sum Y^2$ are the sums of squared X scores and squared Y scores respectively

4.13.2. Regression (Simple Linear Regression Equation):

$$Y = a + bX$$

Where:

Y is the predicted score,

a is the intercept,

b is the slope of the line,

X is the score on the independent variable.

For hypothesis testing using regression, the researcher looked at the significance of the regression model and the individual predictors. The regression equation helped the researcher understands how changes in the independent variables (cybersecurity challenges, factors, awareness, strategies, tools, and deterrence) are associated with changes in the dependent variable (cybersecurity awareness strategy). The researcher simulated the data collected that represents a plausible scenario based on the conceptual framework of the study and performed correlation and regression analysis to test the stated hypotheses.

4.13.3. Correlation

Based on the collected data, the Pearson correlation coefficients were computed with their corresponding p-values for each of the dependent variables with the independent variable "Cybersecurity Awareness Strategy". As follows, are the results:

- **Cybersecurity challenges** and cybersecurity awareness strategy: r = 0.054, p = 0.595
- **Cybersecurity factors** and cybersecurity awareness strategy: r = 0.351, p = 0.00035
- **Cybersecurity awareness** and cybersecurity awareness strategy: r = 0.304, p = 0.0021
- **Cybersecurity strategies** and cybersecurity awareness strategy: r = 0.473, p < 0.0001
- **Cybersecurity tools** and cybersecurity awareness strategy: r = 0.319, p = 0.0012
- **Deterrence** and cybersecurity awareness strategy: r = 0.342, p = 0.00049

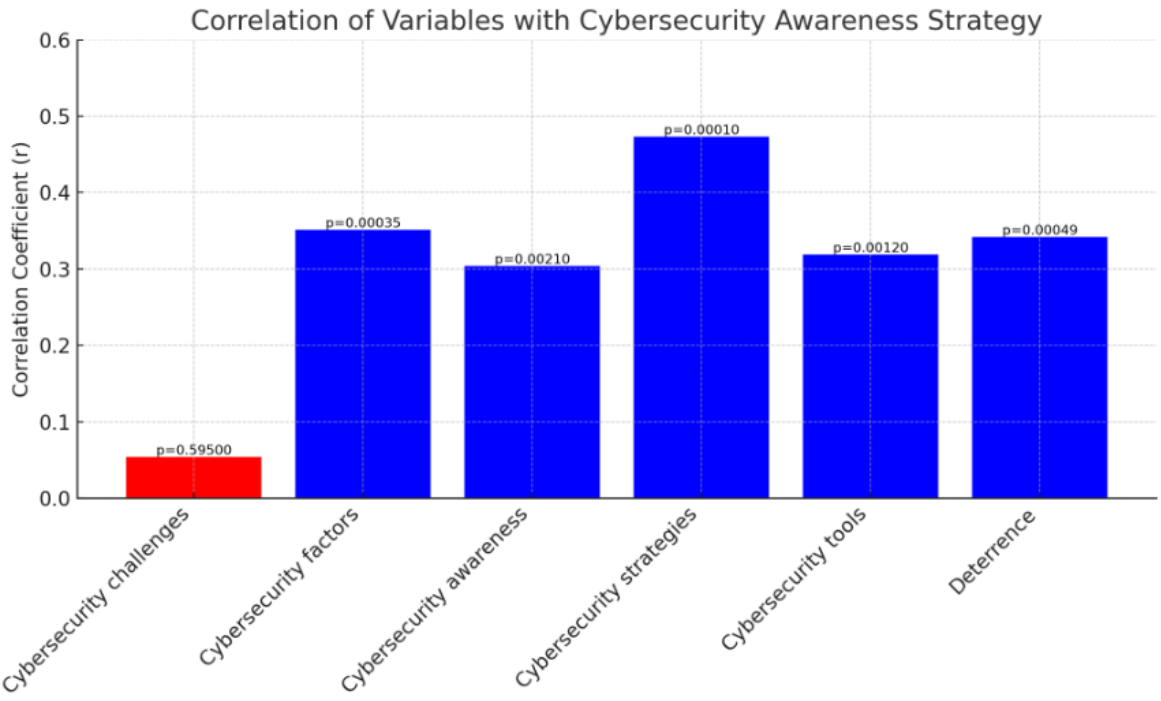

Figure 4.20: Correlation of Variables with Cybersecurity Awareness Strategy

From the above figure 4.20, the relationship between the dependent variables and the cybersecurity awareness strategy is interpreted as follows:

- **Cybersecurity challenges** do not have a statistically significant correlation with the cybersecurity awareness strategy ($p > 0.05$).
- **Cybersecurity factors** show a moderate positive correlation, which is statistically significant ($p < 0.05$).
- **Cybersecurity awareness** exhibits a moderate positive correlation, also statistically significant.
- **Cybersecurity strategies** have a strong positive correlation with the cybersecurity awareness strategy, with high statistical significance.
- **Cybersecurity tools** show a moderate positive correlation, statistically significant.
- **Deterrence** is moderately and positively correlated with the cybersecurity awareness strategy, and the correlation is statistically significant.

The statistical significance ($p < 0.05$) suggests that except for cybersecurity challenges, all other dependent variables have a significant effect on the cybersecurity awareness strategy.

4.13.4. Regression analysis

The regression analysis was conducted to further explore the relationships between the dependent variables (cybersecurity challenges, factors, awareness, strategies, tools, and deterrence) and independent variable (cybersecurity awareness strategy). Regression was employed to assess the impact of all independent variables simultaneously on the cybersecurity awareness strategy.

The results of the multiple regression analysis to assess the impact of the dependent variables on the independent variable "Cybersecurity Awareness Strategy" are as follows:

- **Model Summary**:
    - R-squared: 0.510, indicating that approximately 51% of the variability in the cybersecurity awareness strategy is explained by the model.
    - Adjusted R-squared: 0.478, which adjusts for the number of predictors in the model.
    - F-statistic: 16.10, which tests the null hypothesis that all regression coefficients are equal to zero.
    - Prob (F-statistic): 1.28e-12, indicating that the overall regression model is statistically significant.
- **Coefficients**:
    - **Cybersecurity challenges**: Coefficient = 0.122, p-value = 0.010, suggesting a significant positive influence on the cybersecurity awareness strategy.
    - **Cybersecurity factors**: Coefficient = 0.150, p-value = 0.001, also indicating a significant positive effect.
    - **Cybersecurity awareness**: Coefficient = 0.151, p-value = 0.001, suggesting a significant positive relationship.
    - **Cybersecurity strategies**: Coefficient = 0.207, p-value < 0.001, showing a significant and stronger positive influence.
    - **Cybersecurity tools**: Coefficient = 0.112, p-value = 0.014, indicating a significant positive effect.
    - **Deterrence**: Coefficient = 0.180, p-value < 0.001, indicating a significant positive impact.
- **Other Statistics**:

- Durbin-Watson statistic = 1.745, suggesting that there is no major issue with autocorrelation in the residuals.
- The condition number is 39.7, which is within an acceptable range, indicating that multicollinearity may not be a concern.

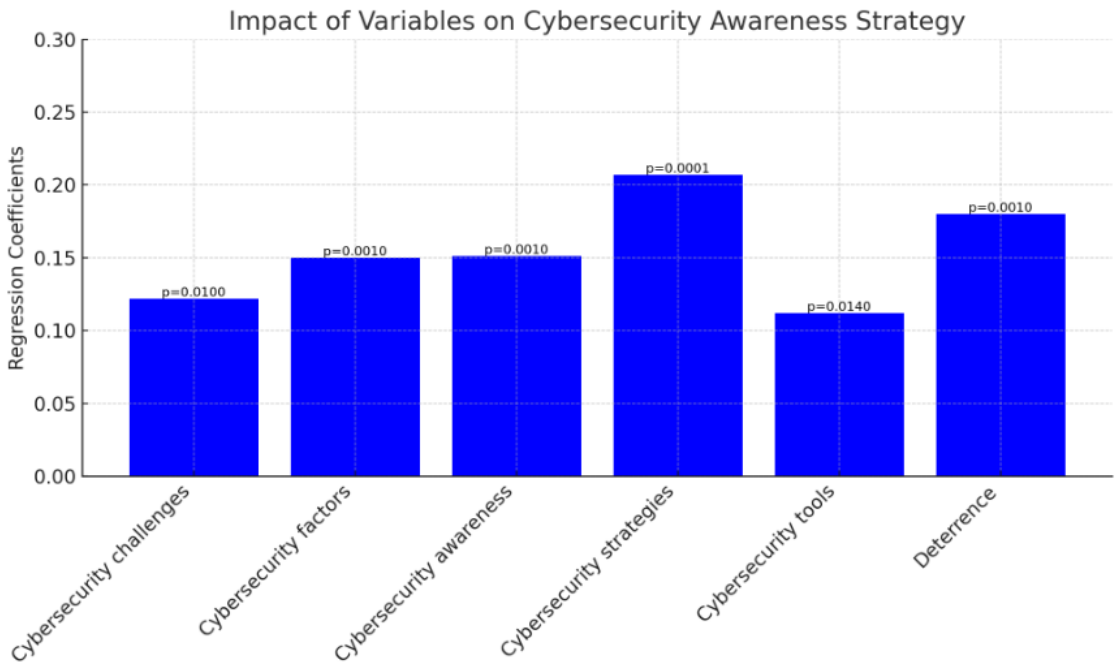

Figure 4.21: Impact of Variables on Cybersecurity Awareness Strategy

The intercept has a coefficient of 0.297 but is not statistically significant (p = 0.354), meaning that when all independent variables are at zero, the expected value of the cybersecurity awareness strategy is 0.297, but this is not a meaningful interpretation in the context of this analysis.

4.14. Interpretation and Analysis of the Hypotheses and Research Questions.

The interpretation and analysis of the hypotheses and research questions were conducted, the researcher delved into the hypotheses and research questions to extract insights and draw conclusive findings based on the statistical analysis of the study (regression and correlation analysis). Through statistical evaluation, the section aimed to explain the relationships between the dependent and independent variables and to validate the hypotheses and research questions.

4.14.1. Hypothesis Outcomes:

- **H1: Cybersecurity challenges influence cybersecurity awareness strategy.**

- The correlation analysis showed a non-significant relationship (r = 0.054, p = 0.595), but the regression analysis showed a positive coefficient that is significant (p = 0.010). This indicates that while cybersecurity challenges may not have a strong linear relationship with cybersecurity awareness strategy, they do have a significant influence when considering other factors.

- **H2: Cybersecurity factors influence cybersecurity awareness strategy.**
  - Both the correlation (r = 0.351, p = 0.00035) and regression analyses (p = 0.001) indicate a significant positive influence. This suggests that factors such as education level and occupation significantly impact cybersecurity awareness strategy in the Mopani District.

- **H3: Cybersecurity awareness influences cybersecurity awareness strategy.**
  - Correlation (r = 0.304, p = 0.0021) and regression (p = 0.001) analyses suggest a significant positive relationship, meaning that higher levels of cybersecurity awareness are associated with more robust cybersecurity awareness strategy.

- **H4: Cybersecurity strategies influence cybersecurity awareness strategy.**
  - This variable showed a strong positive correlation (r = 0.473) and a significant regression coefficient ($p < 0.0001$), implying that existing cybersecurity strategies greatly influence the development and implementation of cybersecurity awareness strategy.

- **H5: Cybersecurity tools influence cybersecurity awareness strategy.**
  - There is a significant moderate positive correlation (r = 0.319, p = 0.0012) and a significant regression coefficient (p = 0.014), indicating that the presence and use of cybersecurity tools are significant predictors of the effectiveness of cybersecurity awareness strategies.

- **H6: Deterrence influences cybersecurity awareness strategy.**
  - The analysis shows a moderate positive correlation (r = 0.342, p = 0.00049) and a significant regression coefficient ($p < 0.001$), suggesting that the belief in cybersecurity measures as a deterrent to cybercrime is an important component of the cybersecurity awareness strategy.

4.14.2. Research Questions Interpretation:

- The cybersecurity challenges faced by rural communities in the Mopani District are significant in shaping cybersecurity awareness strategies, even if their direct correlation is not strong.
- The level of cybersecurity awareness is positively associated with the cybersecurity awareness strategies, indicating that as awareness increases, so does the commitment to and potential effectiveness of these strategies.
- The attitude of rural communities towards cybersecurity, particularly the perception of deterrence, significantly affects the cybersecurity awareness strategies being developed.
- Factors that influence cybersecurity policies include the general awareness of cybersecurity issues, the existing strategies in place, and the practical tools available to the community.
- A suggested cybersecurity awareness strategy for the Mopani District should consider enhancing the understanding of cybersecurity factors, boosting overall awareness levels, leveraging current strategies, and ensuring access to essential cybersecurity tools. It should also emphasise the role of deterrence in combating cyber threats.

4.15. Chapter Summary

In summary, this chapter provided an in-depth analysis of the data gathered from respondents within the rural communities of the Mopani District in the Limpopo Province, specifically in Phalaborwa. The chapter is structured into eight parts, detailing the perspectives of residents in rural areas concerning various aspects. Responses to all questions are presented in either tabular or graphical formats. Furthermore, the analysis highlights key findings related to cybersecurity challenges, awareness levels, attitudes, and factors influencing cybersecurity policies. Notably, the results emphasise the significance of strategies, tools, and deterrence as essential constructs in the adoption of cybersecurity awareness strategies. Furthermore, a regression analysis was performed to determine the extent of influence in predicting the intention to utilise cybersecurity awareness strategies, while correlation analysis elucidated the relationships between the variables. The subsequent chapter presents the main findings aligned with the research questions and the proposed framework.

5. CHAPTER 05: DISCUSSIONS OF FINDINGS AND PROPOSED CYBERSECURITY AWARENESS STRATEGY

5.1. Introduction

The previous chapter thoroughly analysed, presented, and interpreted the data gathered from respondents. This chapter delves into the main research findings from the previous chapter. Its objective is to ascertain whether the research questions outlined in Chapter One have been addressed. Based on the results, the researcher proposes a strategy for cybersecurity awareness for the rural communities of Mopani District of the Limpopo Province.

5.2. Discussion Based on the Findings

The primary aim of the study was to develop a cybersecurity awareness strategy for rural communities of the Mopani District in Limpopo Province and propose the strategy for cybersecurity awareness. The following discussions are based on answering the research questions.

5.2.1. Challenges of Cybersecurity

The frequency of residents experiencing cyberattacks, types of cyberattacks experienced, and cybersecurity challenges were identified through addressing the research question: *What are the cybersecurity challenges faced by rural communities of Mopani District in Limpopo Province?*

5.2.1.1. The Frequency of Residents Experiencing Cyberattacks

The data indicates that a substantial majority of respondents, comprising 81%, have either personally experienced a cyberattack or are acquainted with someone who has encountered such an incident. This high percentage underscores the prevalence and impact of cyberattacks within the surveyed group. Conversely, 19% of respondents stated that they have not personally experienced a cyberattack, nor are they aware of anyone in their network who has faced such an incident. While this percentage is comparatively smaller, it indicates that there is still a segment of the respondents who have not directly encountered or been exposed to cyberattacks. The results emphasise the widespread nature of cyber threats within the community, with a majority of individuals having direct or indirect experiences with cyberattacks. This underscores the urgent need for cybersecurity awareness, education, and measures to mitigate the risks and consequences associated with such incidents in the community.

5.2.1.2. Types of Cyberattacks Experienced

The survey findings unveil the prevalence of cyberattacks among the respondents in the Mopani District. A substantial 81% of respondents reported experiencing a cyberattack themselves or knowing someone who has. This indicates a widespread awareness of the issue within the community. However, 19% of respondents noted that they have not encountered or are unaware of anyone experiencing a cyberattack. Delving into the types of cyberattacks experienced, the results reveal a varied landscape. Phishing emerges as the most common cyber threat, with 34% of respondents citing it as their primary experience. Following closely are malware incidents at 21%, data breaches at 18%, ransomware attacks at 14%, and DDoS attacks at 13%. These statistics underscore the diverse challenges posed by cyber threats in the Mopani District, with phishing being the most prevalent. The collective data emphasises the need for increased cybersecurity awareness and measures to protect individuals and communities from these evolving digital risks.

5.2.1.3. Cybersecurity Challenges

The analysis of cybersecurity challenges in rural communities within the Mopani District reveals a complex landscape. Notably, the lack of cybersecurity emerges as the most prominent challenge, constituting 33% of the responses. This underscores a significant gap in cybersecurity infrastructure and awareness within the community, potentially leaving them vulnerable to various threats. Cybersecurity activities are also highlighted as a substantial challenge, with 24% of respondents expressing concern. This suggests that not only is there a lack of cybersecurity measures, but the existing activities may not be robust or effective in addressing the evolving threat landscape. This finding emphasises the need for comprehensive cybersecurity strategies tailored to the specific needs of these communities.

Furthermore, 20% of respondents identify limited access to cybersecurity resources as a noteworthy challenge. This limitation could hinder the community's ability to implement and maintain effective cybersecurity measures. It points to potential disparities in resource distribution and access, which need attention for a more equitable and secure environment. In addition, 15% of respondents highlight weak or non-existent cybersecurity policies as a concern. This indicates a governance and regulatory gap, emphasising the importance of establishing clear cybersecurity policies to guide practices and behaviors within the community.

Lastly, 8% of respondents express concerns about insufficient cybersecurity training. This finding underscores the critical role of education and awareness in enhancing cybersecurity resilience. Insufficient training could lead to a lack of understanding about potential threats and the necessary precautions, leaving individuals and the community exposed. Collectively, these challenges create an environment conducive to the facilitation or prevalence of

cyberattacks within the Mopani District. Addressing these issues requires a holistic approach that includes improving infrastructure, enhancing cybersecurity activities, ensuring equitable access to resources, establishing robust policies, and providing adequate training and awareness programs tailored to the needs of rural communities.

5.2.2. Factors Influencing Cybersecurity Policies

Awareness of cybersecurity policies or initiatives, types of the cybersecurity policies or initiatives that the residents are aware of, and the factors that influence the development and implementation of cybersecurity policies were identified through addressing the research question: *What are the factors that can influence cybersecurity policies in rural communities?*

5.2.2.1. Awareness of cybersecurity policies or initiatives

The findings reveal a substantial lack of awareness among the respondents regarding local cybersecurity policies or initiatives. A staggering 96% of the respondents indicated that they are unaware of any such policies or initiatives, while a mere 4% expressed awareness. These results point to a significant gap in knowledge and awareness regarding cybersecurity-related measures in the Mopani District. The overwhelming lack of awareness suggests that there may be a dearth of robust campaigns or accessible information regarding various aspects of cybersecurity within the Mopani District. It implies that the community is not well-informed about the existence, content, or significance of local cybersecurity policies or initiatives. Furthermore, these findings raise the possibility that there might be limited, if any, cybersecurity measures in place within the Mopani District, contributing to the prevailing lack of awareness among the respondents.

In essence, the low level of awareness underscores the need for increased efforts in disseminating information, fostering campaigns, and potentially developing and implementing cybersecurity policies in the region. Addressing this informational gap is crucial to enhancing the overall cybersecurity posture of the Mopani District and empowering its residents to navigate the digital landscape with greater awareness and resilience.

5.2.2.2. Types of the cybersecurity policies or initiatives that the residents are aware of.

Public-private partnerships for cybersecurity emerged as the most prominently recognised initiative, with 38 respondents (21.7%) expressing awareness of such collaborations. These partnerships are pivotal in fostering collaborative efforts between government entities and private organizations, contributing significantly to enhancing the overall resilience of cybersecurity measures. The acknowledgment of government-funded cybersecurity programs by 37 respondents (21.10%) underscores the importance of state-sponsored initiatives in fortifying cybersecurity measures. Such programmes typically involve financial support for

cybersecurity initiatives, comprehensive training, and the development of critical cybersecurity infrastructure. Furthermore, respondents recognised the significance of data protection regulations, with 35 individuals (20%) indicating awareness of such policies. These regulations play a vital role in safeguarding individuals' privacy and ensuring responsible handling of sensitive information. The acknowledgment of local cybersecurity awareness campaigns by 35 respondents (20.0%) highlights the crucial role of grassroots efforts in educating the community on cybersecurity matters. These campaigns contribute significantly to building a cyber-resilient community by empowering individuals with knowledge and best practices.

Thirty respondents expressed awareness of local cybersecurity education initiatives, underscoring the importance of educational programs in equipping individuals with the necessary knowledge and skills in cybersecurity. These education initiatives aim to bridge the knowledge gap and empower individuals to navigate the digital landscape securely. Overall, these findings emphasise the multifaceted approach required to bolster cybersecurity awareness and resilience, involving collaborative partnerships, government-sponsored programs, regulatory frameworks, and grassroots educational efforts.

5.2.2.3. Factors that influence the development and implementation of cybersecurity policies

The majority of respondents, comprising 153 individuals (23.6%), underscored the critical role of community engagement and awareness in shaping effective cybersecurity policies. This highlights the significance of actively involving local communities in cybersecurity initiatives and conducting awareness campaigns to enhance understanding and cooperation. The emphasis on community engagement aligns with the notion that building a cyber-resilient environment necessitates the active participation and awareness of the people it seeks to protect. Government support and regulatory frameworks emerged as pivotal factors influencing cybersecurity policy development, as recognised by 149 respondents (23%). Advocacy for government involvement and the establishment of clear regulations to guide cybersecurity practices in rural areas are pivotal considerations. This signifies the importance of a regulatory framework to provide guidance and structure to cybersecurity efforts, especially in rural settings.

Furthermore, 144 respondents (22.3%) highlighted the significance of having access to cybersecurity expertise in rural communities. Addressing this challenge involves the implementation of initiatives such as training programs, knowledge-sharing platforms, and partnerships with cybersecurity professionals. Enhancing expertise within rural communities contributes to building a knowledgeable and skilled populace capable of navigating the evolving cybersecurity landscape. The availability of funding and resources emerged as a

critical factor, with 122 respondents (18.9%) recognising its impact on the development and implementation of cybersecurity policies. Identifying sustainable funding sources and optimising resource allocation are deemed essential components in overcoming this challenge. Adequate financial support is crucial for executing effective cybersecurity strategies and sustaining long-term initiatives.

Lastly, collaboration with local organizations was identified by 78 respondents (12.3%) as a contributing factor in cybersecurity policy development. Building partnerships with local entities can foster a collaborative approach to addressing cybersecurity challenges and leverage shared resources. This collaborative spirit enhances the overall resilience of rural communities against cybersecurity threats and fosters a collective response to the evolving landscape of digital security.

5.2.3. Cybersecurity Awareness

The awareness of cybersecurity concepts, frequency of seeking information about cybersecurity threats and best practices, the type of cybersecurity training or education received, and the efficiency of the cybersecurity training or education received were identified through addressing the research question: *What is the level of cybersecurity awareness among rural communities in the Mopani District of Limpopo Province?*

5.2.3.1. The awareness of cybersecurity concepts, frequency of seeking information about cybersecurity threats and best practices, the type of cybersecurity training or education received, and the efficiency of the cybersecurity training or education received.

In the surveyed population of the Mopani District, the awareness of cybersecurity concepts exhibited considerable variation among respondents. A significant portion, comprising 60.5%, reported being Not Aware. In contrast, 17.5% considered themselves Very Aware, and 10.5% described their awareness as Extremely Aware. The categories of Moderately Aware and Slightly Aware accounted for 7.5% and 4.0%, respectively. Furthermore, when exploring information-seeking habits about cybersecurity, the majority of respondents demonstrated infrequent engagement. A notable 58.50% reported Never actively seeking information, followed by Rarely at 19.50%. A smaller percentage engaged more regularly, with 13.50% choosing Daily, 5.50% Monthly, and 3.00% Weekly.

Regarding the effectiveness of cybersecurity training or education received in rural communities in Mopani, respondents expressed diverse perspectives. The largest group, constituting 54.00%, found the training Not Very Effective, while 13.50% considered it Very Effective. Additional responses included Somewhat Effective (6.00%), Not Effective at All (4.50%), and another 54.00% indicating Not Very Effective. Moving on to the specific

cybersecurity training or education received in rural communities in Mopani, the examination revealed various insights. A significant number of respondents, accounting for 54.5%, indicated that they have not received any specific cybersecurity training or education tailored to the Mopani District. This underscores an opportunity to explore and implement targeted training initiatives to address the current gap in cybersecurity education. Among the respondents who received training, in-person training sessions were recognised by 12.4%, offering direct interaction, opportunities to ask questions, and hands-on activities. Educational materials, such as brochures and pamphlets, were acknowledged by 12.10% as a source of cybersecurity information. Online courses or webinars were cited by 11.1%, indicating a preference for digital learning platforms. Workshops or seminars were identified by 9.9%, offering interactive learning and practical application of cybersecurity principles.

5.2.4. Residents' Attitude towards Cybersecurity

The Residents' attitude towards cybersecurity was identified through addressing the research question: *What is the attitude of rural communities towards cybersecurity?*

In the examined population of the Mopani District, perceptions regarding the importance of cybersecurity demonstrated considerable diversity. A notable 24.50% strongly agreed that cybersecurity is crucial for community safety, indicating a substantial portion with a strong stance. Conversely, a significant 59.50% disagreed, highlighting varying perspectives within the community. The mean score of 3.8, with a standard deviation of 1.676, emphasises the dispersion and central tendency of attitudes. Concerning potential cybersecurity threats, 32.00% strongly agreed, signifying a heightened level of apprehension, while 53.00% strongly disagreed. The mean score of 3.54, with a standard deviation of 1.801, illustrates the varying degrees of concern within the community.

The belief that individuals in the community should be educated about cybersecurity revealed a pronounced sentiment. A substantial 33.00% strongly agreed, emphasising the perceived necessity of cybersecurity education. However, 55.00% strongly disagreed, indicating a significant portion with opposing views. The mean score of 3.54, with a standard deviation of 1.832, highlights the dispersion and central tendency of views on the necessity of cybersecurity education. In terms of community investment in cybersecurity measures and tools, a significant 33.00% strongly agreed, reflecting a proactive stance. However, 52.50% strongly disagreed, showcasing a substantial portion with a reluctance to invest in cybersecurity. The mean score of 3.51, with a standard deviation of 1.816, elucidates the community's varying degrees of willingness to invest in cybersecurity.

Furthermore, a substantial majority (68%) rate the level of awareness about cybersecurity among residents as very low. This underscores the need for comprehensive community-wide

awareness campaigns, with customised strategies addressing local challenges to enhance overall awareness. Only 2% reported a high level of awareness about cybersecurity among residents, indicating a significant gap that needs attention.

5.2.5. Cybersecurity Strategies (Construct)

5.2.5.1. Sources used to rely on for information about cybersecurity, usage of strong, and unique passwords for online accounts, frequency update of software and applications to the latest versions, and cautiousness about clicking on links or attachments in emails from unknown senders was discovered:

The analysis of cybersecurity strategies and awareness reveals several key findings. The notable observation is that a considerable portion of respondents, accounting for 45.8%, does not depend on specific sources for cybersecurity information. This emphasises the need for targeted strategies to reach and educate individuals who currently lack dedicated sources for cybersecurity information. Among those who identified specific sources, the internet emerges as a significant channel, with 16% recognising it as a valuable resource for obtaining cybersecurity information. Social media platforms and informal networks, such as friends and family, also play influential roles as cybersecurity information sources, acknowledged by 14.4% and 13.8% of respondents, respectively. Additionally, formal avenues like workshops and training sessions are identified by 9.6% of respondents.

Regarding cybersecurity strategies, the results indicate potential vulnerabilities in password practices. A significant portion, 66.5% of respondents, reported rarely using strong, unique passwords. This emphasises the need for initiatives that emphasise the importance of adopting robust passwords and implementing secure authentication methods. Similarly, a considerable number of respondents, 57%, reported either never or rarely updating their software and applications to the latest versions. This presents an opportunity for educational efforts aimed at underscoring the importance of timely updates and providing guidance on the update process. Another noteworthy finding is that 74.5% of respondents indicated that they rarely exercise caution when clicking on links or attachments in emails from unknown senders. This underscores the need for initiatives focused on cultivating a culture of caution and awareness regarding phishing threats. By enhancing the community's understanding of potential risks and promoting vigilant behavior, these initiatives can play a pivotal role in elevating the overall security posture of the community.

In summary, the results suggest a need for targeted awareness campaigns, educational initiatives, and training programs. Strategies should include promoting strong password practices, emphasising the importance of timely software updates, and raising awareness

about phishing threats. Tailored interventions can bridge the gaps in cybersecurity knowledge and practices within the community.

5.2.6. Tools (Construct)

5.2.6.1. Usage of any antivirus or anti-malware software on devices, types of firewall protection used for networks, awareness of the usage of encryption to secure data on devices, and types of cybersecurity strategies or tools that are in the Mopani District was discovered:

The findings underscore significant gaps in cybersecurity practices within the Mopani District community. An overwhelming majority, comprising 83% of respondents, does not utilise antivirus or anti-malware software, highlighting the need for widespread adoption of these fundamental cybersecurity tools. Initiatives aimed at promoting the use of these tools can substantially enhance digital security within the community. Furthermore, a notable percentage of respondents (92%) lack any firewall protection on their home network, emphasising the importance of promoting both software and hardware firewall adoption to mitigate potential security risks. The survey reveals that 78% of respondents are not aware of the use of encryption to secure data on their devices, indicating a need for educational efforts on encryption benefits to reinforce data security practices. Additionally, 81% of respondents lack awareness of the availability of cybersecurity tools within their community, suggesting the need for tailored strategies to enhance accessibility and foster a safer digital environment. A significant number of respondents (80.5%) are unaware of any cybersecurity strategies or tools employed in the Mopani District, highlighting the necessity for comprehensive awareness campaigns to inform residents about existing cybersecurity initiatives.

The rates of adoption for various cybersecurity strategies in the Mopani District community are relatively low. For instance, firewalls and intrusion detection systems are adopted by 19%, antivirus and anti-malware software by 18%, employee cybersecurity training programs by 17.5%, regular software updates and patch management by 16.1%, encrypted communication tools by 15.6%, and secure password policies and management by 13.7%. These figures offer insights into the prevalence of specific cybersecurity measures within the community, providing a foundation for future initiatives aimed at strengthening overall cybersecurity resilience.

5.2.7. Deterrence (Construct)

5.2.7.1. Residents' opinion towards implementing effective cybersecurity measures that can deter cybercriminals, and the additional cybersecurity measures that the residents think can serve as a deterrent to cybercriminal activities in Mopani was discovered:

The community's perspectives on the effectiveness of implementing cybersecurity measures in rural areas, particularly in Mopani, reveal a significant disparity in opinions. Approximately 26% of respondents strongly agree with the efficacy of cybersecurity measures in deterring cybercriminals, constituting a considerable segment of the community. In contrast, a substantial majority (56.5%) strongly disagrees with this notion. The absence of responses in the Agree category suggests a polarised perspective on the perceived impact of cybersecurity measures in rural settings like Mopani. Figure 4.18 in chapter 4 illustrated the adoption rates for various cybersecurity enhancement strategies within the Mopani community. Encouraging businesses to adopt stronger cybersecurity practices and promoting multi-factor authentication (MFA) both stand out with adoption rates of 15.7%, reflecting significant community support for initiatives that bolster cybersecurity within local businesses and embrace advanced authentication methods. A notable 15.5% of the community supports the implementation of stricter penalties for cybercriminals, indicating a shared belief in the importance of robust legal measures to deter and punish cybercrime.

Furthermore, the enhancement of local cybersecurity infrastructure receives support from 15.1% of the community; highlighting a recognition of the crucial role that infrastructure plays in safeguarding digital environments. Improved cybersecurity education and awareness programs garner a significant adoption rate of 14.4%, underlining the community's commitment to fostering knowledge and awareness regarding cyber threats. Strengthening local law enforcement's capacity to address cybercrime is endorsed by 13.7% of the community, suggesting a desire for enhanced law enforcement capabilities in tackling cyber threats. Although slightly lower at 10.0%, fostering collaboration between local organizations and government agencies still reflects a degree of community interest in cooperative efforts to address cybersecurity challenges.

5.2.8. Proposed Framework for Cybersecurity Awareness Strategy

The cybersecurity awareness strategy for rural communities was formulated according to the study's findings, addressing the research question: *What cybersecurity awareness strategy can be proposed or is appropriate for rural communities in the Mopani District?*

The question aimed to suggest a cybersecurity awareness strategy for rural communities in the Limpopo Province of South Africa. However, background information regarding cybersecurity tools, strategies, and policies was gathered. The results showed that respondents from rural communities in the Mopani District stated that their communities lacked implemented cybersecurity policies to prevent and mitigate cyberattacks. They also indicated the lack of cybersecurity awareness campaigns within their communities. Furthermore, a significant majority of respondents indicated that they do not utilise any tool such as antivirus

or anti-malware software to protect their networks, underscoring the imperative for community-wide adoption of fundamental cybersecurity tools since this indicates that there is no cybersecurity awareness in place.

Furthermore, the findings revealed that the respondents, comprising 81% of the total, had experienced a cyberattack themselves or being acquainted with someone who had encountered such an incident based. Therefore, a suitable cybersecurity awareness strategy is imperative within rural communities of Limpopo Province in South Africa, and this study implemented one to assist in its successful adoption in the Mopani District.

5.3. Cybersecurity Awareness Strategy for Rural Communities of Mopani District

The proposed strategy encompasses the essential success factors for cybersecurity awareness. These factors and their significant components are illustrated in Figure 5.1. Each of these factors was discussed in the following subsections:

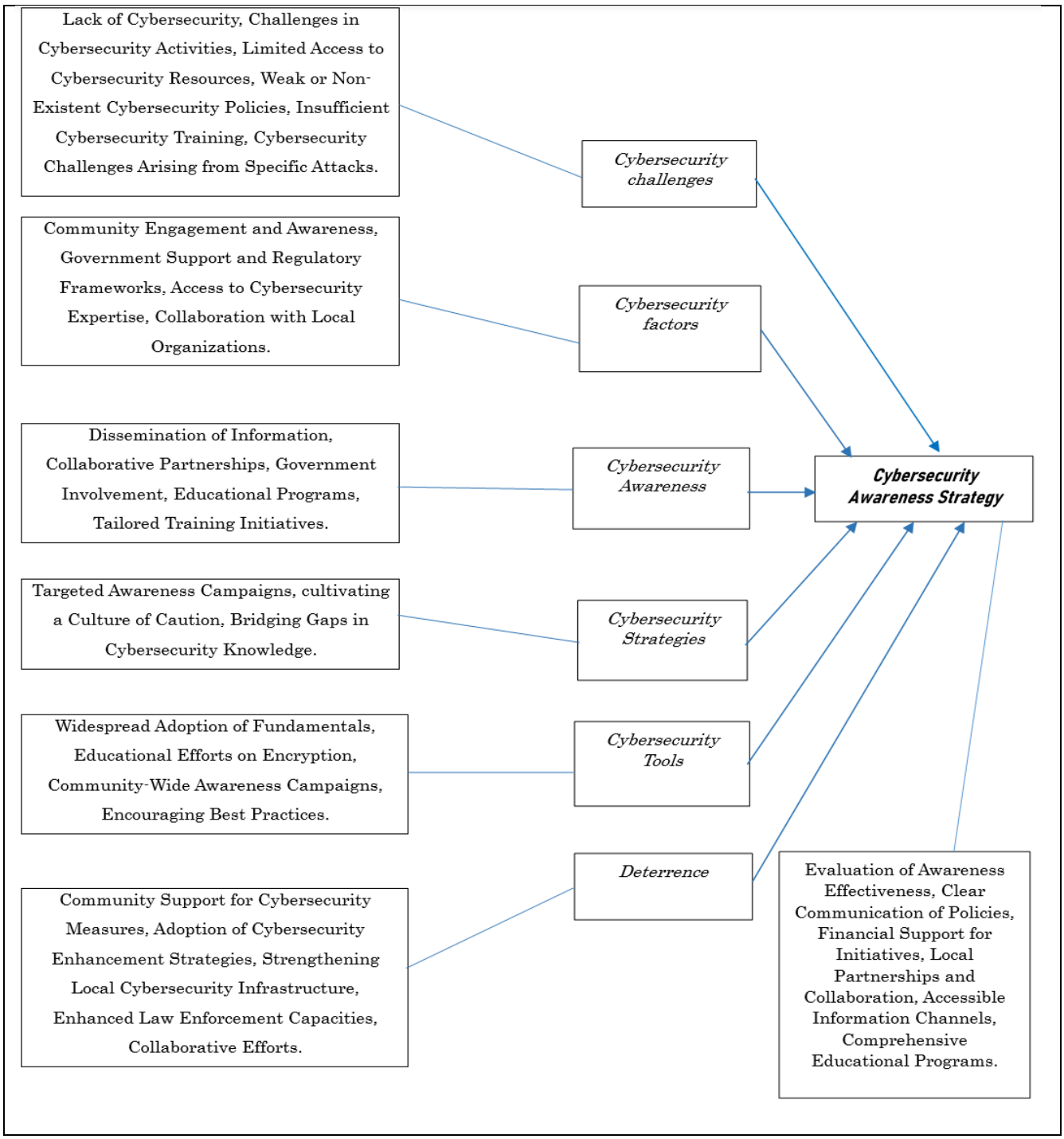

Figure 5.1: Cybersecurity Awareness Strategy for Rural Communities

5.3.1. Cybersecurity Challenges

Cybersecurity challenges, as identified by residents, such as a lack of cybersecurity, limited access to resources, and weak or non-existent policies, directly impact the effectiveness of the cybersecurity awareness strategy. These challenges highlight the existing vulnerabilities that need to be addressed in the awareness programme. Residents identified the lack of cybersecurity (33%), limited access to cybersecurity resources (20%), and weak or non-existent cybersecurity policies (15%) as significant challenges. These responses emphasise the urgency of addressing these challenges in the cybersecurity awareness strategy, since insufficient awareness can result in residents being less vigilant and more susceptible to falling victim to cyberattacks, leading to negative consequences such as data loss and financial harm. Therefore, development of targeted awareness campaigns to address the specific challenges faced by rural communities, focusing on practical and actionable steps, and implementation of educational programs to enhance residents' understanding of common cyber threats and best practices for protection is imperative. The results vary from the studies conducted by Myrmel and Gudmestad (2021) and Chingoriwo (2022) which were concerning the challenges of cybersecurity within rural communities.

5.3.2. Cybersecurity Factors

Both the correlation ($r = 0.351$, $p = 0.00035$) and regression analyses ($p = 0.001$) indicate a significant positive influence on cybersecurity awareness strategy. This suggests that factors such as community engagement and awareness, government support and regulatory frameworks, access to cybersecurity expertise, and collaboration with local organizations significantly impact cybersecurity awareness strategies in the Mopani District. A robust cybersecurity awareness strategy should encompass various cybersecurity factors to adopt a comprehensive approach. By prioritising elements that impact cybersecurity awareness, such a strategy is poised to effectively engage the community, aligning with their comprehension of cybersecurity influences. The identified cybersecurity factors in the study align with those found in previous studies (Wadhwa and Arora, 2017; Wang et al., 2018; Venter et al., 2019; Talukder and Talukder, 2020).

5.3.3. Cybersecurity Awareness

The correlation ($r = 0.304$, $p = 0.0021$) and regression ($p = 0.001$) analyses suggest a significant positive relationship, meaning that higher levels of cybersecurity awareness are associated with more robust cybersecurity awareness strategies. Additionally, the residents' acknowledgment of awareness as a significant challenge emphasises the necessity of tailored strategies. Additionally, studies conducted by Kabanda et al. (2018) and Mashiane et al. (2019) argued that a successful cybersecurity awareness strategy should address the specific

awareness-related challenges faced by rural communities, focusing on education and promoting a culture of cybersecurity (Educational Programs and Tailored Training Initiatives), therefore, tailoring awareness programs (dissemination of information) to the unique challenges encountered in rural communities, emphasising educational initiatives, and fostering a culture of cybersecurity are essential steps in developing a successful cybersecurity awareness strategy.

5.3.4. Cybersecurity Strategies

This variable showed a strong positive correlation ($r = 0.473$) and a significant regression coefficient ($p < 0.0001$), implying that existing cybersecurity strategies greatly influence the development and implementation of cybersecurity awareness strategies. This suggests that a well-developed and executed cybersecurity awareness strategy can positively impact the community's attitude towards cybersecurity through conducting targeted awareness campaigns, cultivating a culture of caution, and bridging gaps in cybersecurity knowledge, and the residents' recognition of limited access to cybersecurity resources as a challenge aligns with the importance of effective strategies. This is supported by Tanner et al. (2018) who stated that tailoring cybersecurity awareness strategies to overcome resource limitations and promoting practical, community-oriented approaches can resonate well with residents.

5.3.5. Cybersecurity Tools

There is a significant moderate positive correlation ($r = 0.319$, $p = 0.0012$) and a significant regression coefficient ($p = 0.014$), indicating that the presence and use of cybersecurity tools are significant predictors of the effectiveness of cybersecurity awareness strategies. Therefore, an effective cybersecurity awareness strategy should strengthen this by emphasising the continued relevance and importance of utilising cybersecurity tools. Furthermore, residents' awareness of the prevalence of phishing attacks emphasises the need for practical guidance on using cybersecurity tools. According to Mashiane et al. (2019), a cybersecurity awareness strategy that educates residents on the specific tools to mitigate phishing risks can enhance their cybersecurity posture. Therefore, incorporating education on specific tools to mitigate phishing risks into a cybersecurity awareness strategy, as suggested by Mashiane et al. (2019), can not only empower residents to enhance their cybersecurity posture, but also empowers them to effectively counteract cyberattacks.

5.3.6. Deterrence

The analysis shows a moderate positive correlation ($r = 0.342$, $p = 0.00049$) and a significant regression coefficient ($p < 0.001$), suggesting that the belief in cybersecurity measures as a deterrent to cybercrime is an important component of the cybersecurity awareness strategy. A cybersecurity awareness strategy should, therefore, incorporate elements of deterrence

such as community support for cybersecurity measures, adoption of cybersecurity enhancement strategies, strengthening local cybersecurity infrastructure, enhanced law enforcement capacities, and collaborative efforts to positively influence the community's attitude towards cybersecurity. Residents' acknowledgment of weak or non-existent cybersecurity policies emphasises the importance of conveying the deterrent aspects of cybersecurity. According to Parn and Edwards (2019), a strategy that emphasises the consequences of cyber threats and the protective role of policies can influence residents' attitudes, therefore emphasising the consequences of cyber threats and the protective role of policies can positively influence residents' attitudes, fostering a stronger commitment to cybersecurity measures and promoting a culture of vigilance and compliance.

5.4. Literature Review and Empirical Evidence

The researcher conducted thorough literature reviews and gathered empirical evidence through questionnaire surveys from respondents to provide comprehensive support for the research objectives. This involved searching existing studies and data relevant to each objective. The aim was to enhance the theoretical framework and empirical foundation of the research. By synthesising findings from diverse sources, the researcher sought to address key gaps in knowledge and contribute to a deeper understanding of cybersecurity challenges, awareness, attitudes, policy factors, and strategic development within rural communities. Furthermore, the integration of both literature and empirical evidence ensured a robust analysis and strengthened the validity of the research findings.

- ***Cybersecurity challenges*** - while literature identifies challenges such as limited technology access and inadequate infrastructure (Smith et al., 2023; Giri and Shakya, 2020), the current study corroborates these findings by revealing specific issues like insufficient cybersecurity training and weak policies in Mopani District.
- ***Cybersecurity awareness*** - literature highlights the need for tailored educational programs (Brown and Lee, 2019; Rahman, Sairi, Zizi, and Khalid, 2020), aligning with the study's findings of low awareness due to limited resources. The research extends this by detailing how these gaps affect local awareness levels.
- ***Cybersecurity attitudes*** - prior studies discuss factors influencing attitudes like perceived risk and trust in technology (Wang et al., 2018; Li et al., 2019). The research both corroborates and extends these findings by revealing mixed attitudes and the influence of local cultural factors.

- ***Influence on cybersecurity policies*** - literature addresses factors like regulations and organizational culture (Young et al., 2018; Humayun et al., 2020), while the study identifies additional factors such as local data protection regulations and community involvement, thus extending the understanding of policy influences.
- ***Cybersecurity awareness strategy*** - effective strategies noted in literature include community-based education and partnerships (Mashiane et al., 2019; Habibzadeh et al., 2019). The study demonstrates the practical application of these strategies through successful local campaigns and partnerships.

5.5. Chapter Summary

The chapter discussed the primary research findings of the study, addressing all research questions aligned with the objectives. Furthermore, the discussion explored challenges, factors, awareness, and attitudes. Additionally, significance was attributed to the role of awareness in fostering the progression of cybersecurity. Lastly, a proposed strategy for cybersecurity awareness was formulated based on the findings.

6. CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

6.1. Introduction

The findings outlined in the fourth chapter and the discussions in chapter five have enabled the researcher to draw conclusions regarding the research study. This chapter highlights the contributions of the research to the existing body of knowledge. Furthermore, it delineates the limitations of the research study. The chapter is intended to underscore recommendations and provide suggestions for potential future research. Lastly, it presents the concluding remarks of the study.

The study has found that implementing cybersecurity awareness strategy is crucial for addressing the unique challenges faced by rural communities. The study also found that the vast majority (121 out of 200, 60.5%) of the residents in the rural communities are unaware of the concept of “cybersecurity”, indicating the urgent need and implementation of cybersecurity awareness strategy for rural communities. Based on the findings of the study, the key conclusions drawn are as follows:

- The study revealed that a majority of the respondents lacked knowledge of cybersecurity (lack of cybersecurity awareness), as a result of limited activities, restricted access to resources, weak policies, and insufficient training, and these primary challenges align with a broader narrative of digital inequity in rural areas. Furthermore, these challenges are not isolated but interconnected, forming a complex landscape that requires comprehensive solutions.
- The findings show that most respondents (residents) were experiencing cyberattacks, particularly phishing incidents.
- The research identified that a majority of the respondents experienced various consequences of cyberattacks, such as data loss, stolen personal information, service disruptions, financial loss, and reputation damage, emphasise the multifaceted and severe repercussions faced by individuals and communities. This information provides a clear picture of the tangible harm resulting from cybersecurity breaches.
- The study found that most respondents had a negative attitude towards the implementation of cybersecurity awareness strategy, however, it might be the reason of the lack of cybersecurity awareness.
- The findings revealed that a majority of respondents (residents), demonstrated awareness of the drivers motivating the need for a cybersecurity awareness strategy in rural communities.

- The findings indicated that respondents acknowledged the positive impacts of a cybersecurity awareness strategy in improving the security environment within rural communities.
- In contrast to general cybersecurity findings, the study highlighted the necessity for tailored awareness strategies specifically designed for the unique challenges faced by rural communities.
- The results found the urgent need to implement a cybersecurity awareness strategy in rural areas, given the prevalence of cyber threats and the potential consequences.
- The study suggests that a strategic focus on quality, community involvement, and addressing specific challenges is essential for the successful implementation of a cybersecurity awareness strategy in rural settings.

6.2. Contribution of the Research Study

- The study significantly contributed to the existing body of knowledge by advancing the theoretical understanding of cybersecurity awareness within the context of South African rural communities, specifically building upon the foundations laid by Game, NIST and Activity theories in information systems. Key determinants influencing cybersecurity awareness and usage were identified, adding valuable insights to the practical implementation of cybersecurity strategies. The study's practical contribution extends to the development of an implementation framework for a cybersecurity awareness strategy, providing a comprehensive guide for rural communities in the Mopani District and other District Municipalities in South Africa. This framework equips decision-makers with the necessary insights to formulate strategic action plans, fostering overall development in the security landscape of rural communities. Furthermore, the research addresses the digital divide by highlighting a significant lack of cybersecurity awareness in these rural settings, emphasising the urgency of targeted awareness initiatives to bridge this gap.
- The study's empirical insights offer a valuable contribution to the field by providing concrete data on cybersecurity challenges in rural contexts. This kind of detailed, localised information is crucial for tailoring effective interventions.
- Highlighting the lack of cybersecurity awareness as a primary challenge is a key contribution. It emphasises the need for not only technological solutions but also educational initiatives to empower residents to recognise and mitigate cyber threats.
- The study's emphasis on weak policies, limited resource access, and the necessity for community-specific strategies and tools contributes to the broader discourse on cybersecurity policy. It signals the importance of considering local nuances in developing and implementing cybersecurity measures.

6.3. Limitations of the Study

The study encountered several limitations that should be acknowledged. Firstly, the sample size was constrained to 200 participants, influenced by the level of access granted by participants. The relatively lower number of participants might be considered a limitation, but recruiting committed volunteers was challenging. Additionally, the exclusion of other South African rural communities beyond Mopani District may affect the generalizability of the results in developing a cybersecurity awareness strategy for rural communities. Furthermore, the study's scope was limited by time and resource constraints, leading to the exclusion of other Districts, Provinces, and international rural communities. This could have enriched the study's results and expanded the researcher's understanding. The suggested strategy, while reviewed for context applicability by project supervisors, was not practically tested within any rural community environment. Another limitation pertains to the data collection method, as only questionnaires with closed-ended questions were used, omitting the richness that could be derived from interviews. The external validity of the study may be compromised due to potential biases introduced by respondents seeking to impress the researcher, resulting in errors. Some participants may have chosen not to engage in the survey due to various reasons, including lack of interest, motivation, or time constraints. Incomplete data, indicated by unanswered questions, may impact the reliability of results. Despite these limitations, the findings offer valuable insights into subjects' preferences, attitudes, and experiences with cybersecurity awareness in rural communities, contributing to the understanding of the overall impact of cybersecurity awareness.

6.4. Recommendations

- It is recommended to consider the enhancement of Cybersecurity Awareness Programmes through the development and implementation of the targeted cybersecurity awareness programs in the Mopani District, specifically tailored to address the identified challenges, such as the lack of awareness and limited access to resources.
- It also recommended to collaborate with local authorities to formulate and implement cybersecurity policies that are specifically designed for rural communities, considering their unique needs and circumstances.
- It is recommended to consider allocations of resources to provide comprehensive cybersecurity training to residents, focusing on building their capacity to recognise and mitigate cyber threats effectively.
- It is also recommended that district municipalities should to consider working with cybersecurity practitioners to develop and deploy user-friendly cybersecurity tools that align with the capabilities and preferences of rural community members.

- It is also recommended that district municipalities should encourage community members to advocate for increased access to cybersecurity resources within the Mopani District, fostering a collaborative effort to improve cybersecurity resilience.
- It is recommended to conduct longitudinal studies to continuously monitor and track changes in cybersecurity challenges and awareness over time, enabling a more dynamic and adaptive approach to addressing emerging threats.
- It is also recommended to expand the scope of research by conducting comparative analyses with other rural districts to identify commonalities and differences in cybersecurity challenges and responses, providing a broader perspective.
- It is also recommended that the local government should foster collaborations between local authorities, cybersecurity practitioners, and private entities to pool resources and expertise, creating a more robust and sustainable cybersecurity ecosystem.
- Lastly, it is suggested that the local government based in the rural communities should regularly evaluate the implementation of the recommended cybersecurity awareness strategy, seeking feedback from stakeholders and adjusting the approach based on lessons learned and changing circumstances and establish a strategy for regular engagement with community members to gather feedback, assess the effectiveness of awareness programs, and identify evolving challenges in real-time.

6.5. Further Research Suggestions

The current study significantly advances understanding of cybersecurity awareness strategy development in South African rural communities, including regions such as Majeje Benfarm, Humulani, Selwane, Makhushane, and Mashishimale. Despite meeting its objectives, there are important areas for future research. Expanding the research to include various districts and rural communities would provide comparative data and address literature gaps. Broadening the geographical scope to encompass diverse South African and international rural communities could enhance generalizability. Future studies should also consider qualitative or mixed-method approaches, using focus groups and interviews with stakeholders to offer nuanced insights and case studies. A longitudinal design is recommended to track changes in cybersecurity awareness strategy over time. This approach would offer a comprehensive understanding of the temporal dynamics in cybersecurity awareness. Additionally, evaluating the success of the developed strategies in other rural communities could provide insights into their performance post-implementation. Future research could test alternative theoretical frameworks, incorporating cultural factors, local government acceptance, and the role of government in cybersecurity awareness. Investigating how theories apply in practical contexts within rural communities would deepen theoretical insights.

Moreover, exploring how cybersecurity policies and governance frameworks, such as NIST, FISMA, and ENISA, impact the development of awareness strategies could offer valuable contributions to theory. Comparative analyses between rural and urban areas with differing cybersecurity adoption rates could reveal significant operational differences and contextual challenges. This exploration would enhance theoretical understanding of the factors influencing cybersecurity awareness and adoption. A proposed cybersecurity awareness strategy, merging the NIST cybersecurity framework, FISMA, and ENISA guidelines, offers a promising direction for investigation. Research focused on understanding how security policies, strategies, and governance influence the development of cybersecurity awareness strategy within rural communities could provide valuable insights. Lastly, a comparative analysis between rural communities with low cybersecurity adoption rates and urban areas, often characterised by higher adoption rates, could elucidate any significant operational differences resulting from cybersecurity awareness. Investigating the reasons for the delay in cybersecurity awareness within South African communities adds depth to understanding the contextual challenges and opportunities.

6.6. Concluding Remarks

The concluding remarks encapsulate the urgency of addressing cybersecurity challenges in rural communities. By highlighting the interconnected nature of awareness, policy, and resources, the research sets the stage for a holistic approach to cybersecurity. The implementation of recommended measures, as suggested, can contribute to building resilient rural cybersecurity ecosystems, ensuring the protection and well-being of community members. This comprehensive approach, combining empirical findings, awareness prioritization, policy implications, and practical recommendations, positions the research as a valuable contribution to the discourse on cybersecurity in rural settings.

7. REFERENCES

Abdulrasool, F.E. and Turnbull, S.J., 2020. Exploring security, risk, and compliance driven IT governance model for universities: applied research based on the COBIT framework. *International Journal of Electronic Banking*, *2*(3), pp.237-265.

Adamopoulou, E. and Moussiades, L., 2020. An overview of chatbot technology. In *IFIP international conference on artificial intelligence applications and innovations* (pp. 373-383). Springer, Cham.

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

Aishwarya, K., Pratiksha, S., Hule, P., & Sayli, M. (2018). Survey on Network security. *International Journal of Current Trends in Science and Technology*, *8*(1), 47-53.

Akhtar, Z., 2021. Malware detection and analysis: Challenges and research opportunities. *arXiv preprint arXiv:2101.08429*.

Akinwumi, D.A., Iwasokun, G.B., Alese, B.K. and Oluwadare, S.A. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology*, *36*(4), pp.1271-1285.

Al Faruq, B., Herlianto, H.R., Simbolon, S.H., Utama, D.N. and Wibowo, A., 2020. Integration of ITIL V3, ISO 20000 & iso 27001: 2013forit services and security management system. *International Journal*, *9*(3).

Zamora, J. (2020). Managing AI within a digital density framework. In J. Canals & F. Heukamp (Eds.), The future of management in an AI world (pp. 201-215). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-20680-2_11.

Al-Ashmoery, Y., Haider, H., Haider, A., Nasser, N. and Al-Sarem, M., 2021, December. Impact of IT Service Management and ITIL Framework on the Businesses. In *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)* (pp. 1-5). IEEE.

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Anders, S.B., 2019. COSO's Newest ERM Guidance. *The CPA Journal*, *89*(3), pp.66-67.

Angelini, M., Lenti, S. and Santucci, G., 2017, October. Crumbs: a cyber security framework browser. In *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)* (pp. 1-8). IEEE.

Asamoah, H., 2020. Antivirus software versus malware. *Архів кваліфікаційних робіт*.

Bada, M., Solms, B. and Agrafiotis, I., (2019). Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *International Journal on Advances in Security*, *12*(2), 108–118.

Ba-Phalaborwa Municipality Draft IDP (2021-2022). *Final 2022-23 IDP*. Retrieved from: https://www.phalaborwa.gov.za/docs/idp/2021-22%20DRAFT%20IDP08042021.pdf.

Baporikar, N., 2020. Strategy for ICT adoption in SMEs. In *Handbook of Research on Increasing the Competitiveness of SMEs* (pp. 244-259). IGI Global.

Breslin, D. and Gatrell, C., 2023. Theorizing through literature reviews: The miner-prospector continuum. *Organizational Research Methods*, *26*(1), pp.139-167.

Clim, A., (2019). Cyber security beyond the industry 4.0 era. A short review on a few technological promises. Informatica Economica, 23(2), pp.34-44.

Brink, H., Van der Walt, C. and Van Rensburg, G., 2018. *Fundamentals of research methodology for health care professionals*. (4th Edition).

Brown, R. and Lee, R.M., (2019). *The evolution of cyber threat intelligence (cti): 2019 sans cti survey*: *SANS Institute.* Retrieved from: https://www. sans. org/white-papers/38790/(accessed on 12 July 2021).

Burns, E. and Brush, K., (2021). What is deep learning and how does it work. *SearchEnterpriseAI*.

Carlos, A., 2021. IT governance as drivers of dynamic capabilities to gain corporate performance under the effects of environmental dynamism. *International Journal of Business*, *8*(3), pp.181-206.

Cavico, F. J. and Mujtaba, B. G. (2017). Wells Fargo's fake accounts scandal and its legal and ethical implications for management. *SAM Advanced Management Journal*, *82*(2), 4.

Chang, L.Y. and Coppel, N., 2020. Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*, p.101959.

Chikalova, S.V., Tkachuk, P.R. and Lavrinenko, M.D., 2021. Evolution of computer viruses.

Choi, K.S., Cho, S. and Lee, J.R., 2019. Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior*, *100*, pp.1-10.

Chukwudi, A. E., Udoka, E. and Charles, I., (2017). Game theory basics and its application in cyber security. *Advances in Wireless Communications and Networks*, *3*(4), 45-49.

Cisco, J., (2020). Using academic skill set interventions to reduce impostor phenomenon feelings in postgraduate students. *Journal of Further and Higher Education*, *44*(3), pp.423-437.

Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A., 2022. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, p.103614.

Correia, S., 2021. Cybercrime victims: Victim policy through a vulnerability lens. *Available at SSRN 3897927*.

Creswell, J.W. and Creswell, J.D., 2018. Research Design: Qualitative, Qualitative and Mixed Methods Approaches. (5th Ed). London. *SAGE Publication Inc.*

CSIR. (2011). Our future through science: Annual report. Retrieved from https://researchspace.csir.co.za/dspace/bitstream/handle/10204/11851/CSIR%20Annual%20Report_2011-12.pdf?sequence=1&isAllowed=y

Culot, G., Fattori, F., Podrecca, M. and Sartor, M., 2019. Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, *47*(3), pp.79-86.

CyberVentures., (2019). CyberVentures Cybercrime Report. In *Herjavec Group*. *Enterprises in Kenya and Small and Medium*. (n.d.).

Dan Perbankan, J.K., 2021. COSO ERM Framework as the Basis of Strategic Planning in Islamic Banking. *Jurnal Keuangan Dan Perbankan*, *25*(1), pp.21-35.

Dangi, M.R.M., Nawawi, A. and Salin, A.S.A.P., 2020. Application of COSO framework in whistle-blowing activities of public higher-learning institutions. *International Journal of Law and Management*, *62*(2), pp.193-211.

De Doncker, K. and McLean, N., 2022. Social media, sleep difficulties and depressive symptoms: A case study of South African youth in Cape Town. *Technology in Society*, *70*, p.102038.

Deora, R.S. and Chudasama, D., 2021. Brief study of cybercrime on an internet. *Journal of Communication Engineering & Systems*, *11*(1), pp.1-6.

Filiz, B., Arief, B., Cetin, O. and Hernandez-Castro, J., 2021. On the effectiveness of ransomware decryption tools. *Computers & Security*, *111*, p.102469.

Garcia, I., Pacheco, C., Leon, A. and Calvo-Manzano, J.A., 2020. A serious game for teaching the fundamentals of ISO/IEC/IEEE 29148 systems and software engineering–Lifecycle processes–Requirements engineering at undergraduate level. *Computer Standards & Interfaces*, *67*, p.103377.

Geer, D., Jardine, E. and Leverett, E., 2020. On market concentration and cybersecurity risk. *Journal of Cyber Policy*, *5*(1), pp.9-29.

Gilkes, S., (2022). *The Applicability of Game Theory in Cybersecurity Defense Decision-Making* (Doctoral dissertation, Utica University).

Giri, S. and Shakya, S., 2020. High Risk of Cybercrime, Threat, Attack and Future Challenges in Nepal. *International Journal of Computer Sciences and Engineering*, *8*(2), pp.46-51.

Gonzalez III, J.J. and Kemp, R.L. eds., 2019. *Cybersecurity: Current Writings on Threats and Protection*. McFarland.

Gordon, L.A., Loeb, M.P. and Zhou, L., 2020. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), p.tyaa005.

Goutam, R.K., 2021. *Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals (English Edition)*. BPB Publications.

Gunawan, H., 2019, August. Strategic management for it services using the information technology infrastructure library (ITIL) framework. In *2019 international conference on information management and technology (ICIMTech)* (Vol. 1, pp. 362-366). IEEE.

Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B. and Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, p.101660.

Halouzka, K., Kozak, P., Buřita, L. and Matoulek, P., 2021, June. Personal cyber security in email communication. In *2021 International Conference on Military Technologies (ICMT)* (pp. 1-5). IEEE.

Hamdani, S.W.A., Abbas, H., Janjua, A.R., Shahid, W.B., Amjad, M.F., Malik, J., Murtaza, M.H., Atiquzzaman, M. and Khan, A.W., 2021. Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. *ACM Computing Surveys (CSUR)*, *54*(3), pp.1-36.

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, p.102726.

Heidt, M. and Gerlach, J.P., (2019). Investigating the Security Divide Between and Large Companies: How rural communities' characteristics Influence Organisational IT Security Investments. Inf. Syst. 1285-1305.

Hodges, S., Sentance, S., Finney, J. and Ball, T., 2020. Physical computing: A key element of modern computer science education. *Computer*, *53*(4), pp.20-30.

Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, pp.3171-3189.

Jain, Y., Tiwari, N., Dubey, S. and Jain, S., 2019. A comparative analysis of various credit card fraud detection techniques. *International Journal Recent Technology Engineering*, *7*(5S2), pp.402-407.

Jaravel, X. and O'Connell, M., (2020). Real-time price indices: Inflation spike and falling product variety during the Great Lockdown. *Journal of Public Economics*, *191*, 104270.

Jiao, R., Commuri, S., Panchal, J., Milisavljevic-Syed, J., Allen, J.K., Mistree, F. and Schaefer, D., 2021. Design engineering in the age of industry 4.0. *Journal of Mechanical Design*, *143*(7), p.070801.

Stewart, C.A., Simms, S., Plale, B., Link, M., Hancock, D.Y. and Fox, G.C., 2010, October. What is cyberinfrastructure. In *Proceedings of the 38th annual ACM SIGUCCS fall conference: navigation and discovery* (pp. 37-44).

Kabanda, S., Tanner, M. and Kent, C., (2018). Exploring rural community cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), pp.269-282.

Kamal, S.S.L.B.A., 2019. Research paradigm and the philosophical foundations of a qualitative study. *PEOPLE: International Journal of Social Sciences*, *4*(3), pp.1386-1394.

Kim, Y. and Crowston, K., 2011. Technology adoption and use theory review for studying scientists continued use of cyber-infrastructure. *Proceedings of the American Society for Information Science and Technology*, *48*(1), pp.1-10.

Kumar. R. 2018. Research Methodology: Step by Step Guide for Beginners. (3rd Ed). London: SAGE Publishers.

Kure, H.I., Islam, S. and Razzaque, M.A., (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), p.898.

Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P. and Gourisetti, S.N.G., 2020, October. Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. In *2020 Resilience Week (RWS)* (pp. 106-112). IEEE.

Lee, B. and Paek, S.Y., 2020. Phishing and Financial Manipulation. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp.899-916.

Lee, E., Seo, Y.D., Oh, S.R. and Kim, Y.G., (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials*, *23*(2), pp.1020-1047.

Lee, I., 2021. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), pp.659-671.

Lessambo, F.I., 2023. The Cybersecurity Counteroffensive. In *Anti-Money Laundering, Counter Financing Terrorism and Cybersecurity in the Banking Industry: A Comparative Study within the G-20* (pp. 11-32). Cham: Springer Nature Switzerland.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, pp.13-24.

Mabaso, M. and Kumar, P., (2018). A dual band patch antenna for Bluetooth and wireless local area networks applications. *International Journal of Microwave and Optical Technology*, *13*(5), pp.393-400.

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.S. and Zeineddine, H., 2019. An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*, *7*, pp.93010-93022.

Marti, G., Nielsen, F., Bińkowski, M. and Donnat, P., (2021). A review of two decades of correlations, hierarchies, networks and clustering in financial markets. *Progress in information geometry: Theory and applications*, 245-274.

Maschler, M., Zamir, S. and Solan, E., 2020. *Game theory*. Cambridge University Press.

Mashiane, T., Dlamini, Z. and Mahlangu, T., 2019, February. A rollout strategy for cybersecurity awareness campaigns. In *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa* (pp. 243-250).

Mbamaluikem, P.O. and Ogunyemi, J., 2022. A WIFI-BASED SMART SECURITY SYSTEM.

McAfee, N., (2018). Feminist philosophy.

McGuire, M.R., 2022. Crime, Control and the Ambiguous Gifts of Digital Technology. *The SAGE Handbook of Digital Society*, p.35.

Minnaar, A., 2019. Cybercriminals, cyber-extortion, online blackmailers and the growth of ransomware. *Acta Criminologica: African Journal of Criminology & Victimology*, *32*(2), p.105.

Mishra, S.B. and Alok, S., 2022. Handbook of research methodology [White paper].

Moagar-Poladian, S., Dumitrescu, G. C. and Tanase, I. A., (2017). Retail e-Commerce (E-tail)-evolution, characteristics and perspectives in China, the USA and Europe. *Global Economic Observer*, *5*(1), 167.

Nagyfejeo, E. and Von Solms, B., 2020. Why do national cybersecurity awareness programmes often fail. *International Journal of Information Security and Cybercrime*, *9*(2), pp.18-27.

Nanjundeswaraswamy, T.S. and Divakar, S., 2021. Determination of sample size and sampling methods in applied research. *Proceedings on engineering sciences*, *3*(1), pp.25-32.

Ndung'u, N. and Signé, L., 2020. The Fourth Industrial Revolution and digitization will transform Africa into a global powerhouse. *Foresight Africa Report*, *5*(1), pp.1-177.

Ngoma, M.L., Keevy, M. and Rama, P., 2021. Cyber-security awareness of South African state-mandated public sector organisations. *Southern African Journal of Accountability and Auditing Research*, *23*(1), pp.53-64.

Niselow, T., 2018. Five massive data breaches affecting South Africans. *Mail & Guardian*, *19*.

Nkurunziza, A.S., 2021. *A Framework for Cybersecurity Risk Management: A Case of ICT SMEs in Nairobi, Kenya* (Doctoral dissertation, United States International University-Africa).

Nord, J.H., Koohang, A. and Paliszkiewicz, J., 2019. The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, pp.97-108.

Osman, A.M.S., 2019. A novel big data analytics framework for smart cities. *Future Generation Computer Systems*, *91*, pp.620-633.

Park, Y.S., Konge, L. and Artino, A.R., 2020. The positivism paradigm of research. *Academic Medicine*, *95*(5), pp.690-694.

Parn, E.A. and Edwards, D., 2019. Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*.

Patala, N.N., (2019). *Cybersecurity framework for cloud computing adoption in rural based tertiary institutions*, UNIVEN research space.

Pham, H. C., Brennan, L. and Furnell, S., (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*, *46*, 96-107.

Rahman, N.A.A., Sairi, I., Zizi, N.A.M. and Khalid, F., 2020. The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), pp.378-382.

Rana, B., Singh, Y. and Singh, P.K., 2021. A systematic survey on internet of things: Energy efficiency and interoperability perspective. *Transactions on Emerging Telecommunications Technologies*, *32*(8), p.e4

Richardson, M.D., Lemoine, P.A., Stephens, W.E. and Waller, R.E., 2020. Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), pp.23-39.

Rubio, F., Valero, F. and Llopis-Albert, C., 2019. A review of mobile robots: Concepts, methods, theoretical framework, and applications. *International Journal of Advanced Robotic Systems*, *16*(2), p.1729881419839596.

Saunders, M., Lewis, P. and Thornhill, A., 2019. Research Methods for Business Students Eight Edition. *QualitativeMarket Research: An International Journal*.

Sen, A., Jena, G., Jena, S. and Devabalan, P., 2022. A Case Study on Defending against Cyber Crimes. *Journal of Pharmaceutical Negative Results*, pp.1931-1938.

Shukla, A., Katt, B., Nweke, L.O., Yeng, P.K. and Weldehawaryat, G.K., 2022. System security assurance: A systematic literature review. *Computer Science Review*, *45*, p.100496.

Siponen, M., Soliman, W. and Vance, A., 2022. Common misunderstandings of deterrence theory in information systems research and future research directions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *53*(1), pp.25-60.

Śledziewska, K. and Włoch, R., 2021. *The economics of digital transformation: The disruption of markets, production, consumption, and work*. Routledge.

Smith, K.T., Smith, L.M., Burger, M. and Boyle, E.S., 2023. Cyber terrorism cases and stock market valuation effects. *Information & Computer Security*.

Sonowal, G. and Sonowal, G., 2022. Introduction to phishing. *Phishing and Communication Channels: A Guide to Identifying and Mitigating Phishing Attacks*, pp.1-24.

Soomro, A.N., Kumar, J. and Kumari, J., 2022. The dynamic relationship between FDI, ICT, trade openness, and economic growth: Evidence from BRICS countries. *The Journal of Asian Finance, Economics and Business*, *9*(2), pp.295-303.

Srivastava, A.K., Venkataramanan, V. and Hauser, C., 2023. *Cyber Infrastructure for the Smart Electric Grid*. John Wiley & Sons.

Steuperaert, D., 2019. COBIT 2019: A significant update. *EDPACS*, *59*(1), pp.14-18.

Storck, C.R. and Duarte-Figueiredo, F., 2020. A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE access*, *8*, pp.117593-117614.

Taherdoost, H., 2022. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), p.2181.

Talukder, S. and Talukder, Z., 2020. A survey on malware detection and analysis tools. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *12*.

Tam, T., Rao, A. and Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, p.102385.

Teoh, C.S., Mahmood, A.K. and Dzazali, S., 2017. Is NIST CSF applicable for developing nations? A case study on Government Sector in Malaysia.

GOV.UK., (2020). Coronavirus (COVID-19) in the UK.

Varghese, G., & Xu, J. (2022). *Network Algorithmics: an interdisciplinary approach to designing fast networked devices*. Morgan Kaufmann.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M. and Anderla, A., 2019, March. Credit card fraud detection-machine learning methods. In *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-5). IEEE.

Varpio, L., Paradis, E., Uijtdehaage, S. and Young, M., 2020. The distinctions between theory, theoretical framework, and conceptual framework. *Academic Medicine*, *95*(7), pp.989-994.

Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A., 2019. Cyber security education is as essential as “the three R's”. *Heliyon*, *5*(12), p.e02855.

Wadhwa, A., & Arora, N. (2017). A Review on Cyber Crime: Major Threats and Solutions. *International Journal of Advanced Research in Computer Science*, *8*(5).

Wang, G., Wei, Y., Qiao, S., Lin, P., & Chen, Y. (2018). *Generalised inverses: theory and computations* (Vol. 53). Singapore: Springer.

Wekunda, P.W., Aduda, D.S.O. and Guyah, B. (2021). Determinants of tuberculosis treatment interruption among patients in Vihiga County, Kenya. *Plos one*, *16*(12), p.e0260669.

Yeng, P.K., Szekeres, A., Yang, B. and Snekkenes, E.A., 2021. Mapping the psychosocialcultural aspects of healthcare professionals’ information security practices: Systematic mapping study. *JMIR human factors*, *8*(2), p.e17604.

Young, H., van Vliet, T., van de Ven, J., Jol, S., & Broekman, C. (2018). Understanding human factors in cyber security as a dynamic system. In Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17− 21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA 8 (pp. 244-254). Springer International Publishing.

Yuan, J., 2022. Rethinking the Guiding Significance of COSO-ERM for Enterprise Risk Management in the Post-epidemic Era. *International Journal of Social Science and Education Research*, *5*(6), pp.418-425.

Nguyen, T. M., & Chib, A. (2019). Cybersecurity and Social Media in Southeast Asia: Awareness, Practices, and Policy Implications. Asian Journal of Communication, 29(4), 273-287.

Zevenet. (2022). 7 reasons Zevenet is the best load balancing software in 2022. Zevenet.

Zuo, J., Guo, Z., Gan, J. and Lu, Y., 2021, October. Enhancing Continuous Service of Information Systems Based on Cyber Resilience. In *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)* (pp. 535-542). IEEE.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N., 2022. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), pp.82-97.

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.

Myrmel, L.B.H, Gudmestad, O.T, 2021. Cybersecurity for cities and rural areas in the Arctic region. *ISOPE-I21-1284.*

Chingoriwo, T., 2022. Cybersecurity Challenges and Needs in The Context of Digital Development in Zimbabwe. *Vol. 3 NO. 2(2022). British Journal of Multidisciplinary and Advanced Studies.*

ANNEXURE A: ETHICAL CLEARANCE

ETHICS APPROVAL CERTIFICATE

RESEARCH AND INNOVATION
OFFICE OF THE DIRECTOR

NAME OF RESEARCHER/INVESTIGATOR:
Mr PW Masilane

STUDENT NO:
18019432

PROJECT TITLE: **Cybersecurity Awareness Strategy for rural communities: A Case Study of the Mopani District in the Limpopo Province.**

ETHICAL CLEARENCE NO: **FMCL/23/BIS/04/0505**

SUPERVISORS/ CO-RESEARCHERS/ CO-INVESTIGATORS

NAME	INSTITUTION & DEPARTMENT	ROLE
Prof. A Kadyamatimba	UNIVEN, Business Information Systems	Supervisor
Mr. S Madzvamuse	UNIVEN, Business Information Systems	Co- Supervisor
Mr PW Masilane	UNIVEN, Business Information Systems	Investigator – Student

Type: **Master's Research**
Risk: **Minimal risk to humans, animals, or environment (Category 2)**
Approval Period: **May 2023 – May 2024**

The Research Ethics Social Sciences Committee (RESSC) hereby approves your project as indicated above.

General Conditions
While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, please note the following.

- The project leader (principal investigator) must report in the prescribed format to the REC:
  - Annually (or as otherwise requested) on the progress of the project, and upon completion of the project.
  - Within 48hrs in case of any adverse event (or any matter that interrupts sound ethical principles) during the course of the project.
  - Annually a number of projects may be randomly selected for an external audit.
- The approval applies strictly to the protocol as stipulated in the application form. Would any changes to the protocol be deemed necessary during the course of the project, the project leader must apply for approval of these changes at the REC. Would there be deviated from the project protocol without the necessary approval of such changes, the ethics approval is immediately and automatically forfeited.
- The date of approval indicates the first date that the project may be started. Would the project have to continue after the expiry date; a new application must be made to the REC and new approval received before or on the expiry date.
- In the interest of ethical responsibility, the REC retains the right to:
  - Request access to any information or data at any time during the course or after completion of the project,
  - To ask further questions; Seek additional information; Require further modification or monitor the conduct of your research or the informed consent process.
  - withdraw or postpone approval if:
  - Any unethical principles or practices of the project are revealed or suspected.
  - It becomes apparent that any relevant information was withheld from the REC or that information has been false or misrepresented.
  - The required annual report and reporting of adverse events was not done timely and accurately,
  - New institutional rules, national legislation or international conventions A it necessary

ISSUED BY:
UNIVERSITY OF VENDA, RESEARCH ETHICS COMMITTEE
Date Considered: April 2023

Name of the RESSC Chairperson of the Committee: Prof TS Mashau

Signature

UNIVERSITY OF VENDA
OFFICE OF THE DIRECTOR
RESEARCH AND INNOVATION
2023 -05- 05
Private Bag X5050
Thohoyandou 0950

University of Venda
PRIVATE BAG X5050, THOHOYANDOU, 0950, LIMPOPO PROVINCE, SOUTH AFRICA
TELEPHONE (015) 962 8504/8313 FAX (015) 962 9060
"A quality driven financially sustainable, rural-based Comprehensive University"

ANNEXURE B: QUESTIONNAIRE

CYBERSECURITY AWARENESS STRATEGY FOR RURAL COMMUNITIES: A CASE STUDY OF THE MOPANI DISTRICT IN THE LIMPOPO PROVINCE.

SECTION A: Demographics Information

For each item below, please indicate your answer by putting a cross (X) in the relevant block (please choose only one response in each question).

1. What is your age group?	2. What is your gender?
o 16-25 o 26-35 o 36-45 o 45+	o Male o Female o Other o Prefer not to answer
3. What is your race?	4. What is your Educational Level?
o African/Black o Coloured o Asian/Indian o White	o Degree o Diploma o Grade 12 o Postgraduate o Other
5. What is your Occupation?	6. What are your Years of Residence in Mopani District?
o Employed o Unemployed o Student	o less than 5 o 5-10 o 10+

SECTION B: Cybersecurity Challenges

7. Have you or someone you know experience a cyberattack in the Mopani District?

- ○ Yes, o No

8. If yes, please select the type of cyberattack(s) experienced, (Select all that apply):

☐ Malware infection.

Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system.

☐ Ransomware attack.

A type of malware that encrypts a victim's data, demanding payment for the decryption key.

☐ Phishing attack.

A fraudulent attempt to obtain sensitive information by posing as a trustworthy entity, often through email.

☐ DDoS attack.

A Distributed Denial of Service attack, where multiple systems overwhelm a targeted server, causing service disruption.

☐ Data breach.

The unauthorized access and exposure of sensitive, protected, or confidential data.

☐ Other (please specify) _____

9. What was the impact of the cyberattack(s) on your or the person's affected system/network? (Select all that apply):

☐ Data loss.

☐ Financial loss.

☐ Disruption of services.

☐ Stolen personal information.

☐ Reputation damage.

☐ Other (please specify) _____

10. In your opinion, what are the most significant cybersecurity challenges faced by rural communities in Mopani District? (Select all that apply).

☐ Lack of cybersecurity awareness.

☐ Limited access to cybersecurity resources.

☐ Insufficient cybersecurity training.

☐ Cybercriminal activities.

☐ Weak or non-existent cybersecurity policies.

☐ Other (please specify): _____

SECTION C: Factors Influencing Cybersecurity Policies

11. Are you aware of any local cybersecurity policies or initiatives in the Mopani District?

- o Yes, o No

12. If yes, can you please select the cybersecurity policies or initiatives you are aware of in the Mopani District:

☐ Data protection regulations.

☐ Local cybersecurity awareness campaigns.

☐ Government-funded cybersecurity programs.

☐ Public-private partnerships for cybersecurity.

☐ Local cybersecurity education initiatives.

☐ Other (please specify) _____

13. What factors do you believe influence the development and implementation of cybersecurity policies in rural communities like Mopani?

☐ Government support and regulations.
☐ Community engagement and awareness.
☐ Availability of cybersecurity expertise.
☐ Funding and resources.
☐ Collaboration with local organizations.
☐ Other (please specify): _____

SECTION D: Cybersecurity Awareness

14. On a scale of 1 to 5, how would you rate your awareness of cybersecurity concepts?

(1 = Not Aware, 2 = Slightly Aware, 3 = Moderately Aware, 4 = Very Aware, 5 = Extremely Aware)

15. How often do you actively seek information about cybersecurity threats and best practices?

- Daily
- Weekly
- Monthly
- Rarely
- Never

16. Can you please select the type of cybersecurity training or education you received specific to rural communities in Mopani:

☐ Workshops or seminars.

☐ Online courses or webinars.

☐ In-person training sessions.

☐ Educational materials (e.g., brochures, pamphlets).

☐ Non-received.

☐ None of the above (please specify) _____

17. If received any, how effective did you find the cybersecurity training or education you received in rural communities in Mopani?

- Very Effective.
- Somewhat Effective.
- Not Very Effective.
- Not Effective at All.

SECTION E: Rural Communities' Attitude towards cybersecurity

18. Can you please rate your level of agreement with the following statements regarding cybersecurity in rural communities. (Choose one for each statement):

Statement(s)	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Cybersecurity is important for the safety of our community					
I am concerned about the potential cybersecurity threats that affect our community					
I believe that individuals in our community should be educated about cybersecurity.					
Our community should invest in cybersecurity measures and tools					

19. How would you rate the level of awareness about cybersecurity among residents in our rural community?

- Very High.
- High.
- Moderate.
- Low.
- Very Low.

SECTION F: Cybersecurity Strategies (Construct)

20. What sources do you rely on for information about cybersecurity?

- Internet.
- Workshops/Training
- Social Media.
- Friends/Family.
- None.

- o Other (please specify): _____

21. Do you use strong, unique passwords for your online accounts?

- o Always.
- o Often.
- o Rarely.
- o Never.

22. How frequently do you update your software and applications to the latest versions?

- o Always.
- o Often.
- o Rarely.
- o Never.

23. Are you cautious about clicking on links or attachments in emails from unknown senders?

- o Always.
- o Often.
- o Rarely.
- o Never.

SECTION G: Cybersecurity Tools (Construct)

24. Do you use any antivirus or anti-malware software on your devices?

- o Yes, o No

25. What type of firewall protection do you have on your home network?

- o Hardware Firewall.
- o Software Firewall.
- o No Firewall.

26. Are you aware of the use of encryption to secure data on your devices?

- Yes, o No

27. Is there access to cybersecurity tools (e.g., antivirus software) within your community?

- Yes, o No

28. Are you aware of any cybersecurity strategies or tools used in the Mopani District to enhance online security?

- Yes, o No

29. If yes, please select the specific cybersecurity strategies or tools you are aware of in the Mopani District:

- Firewalls and intrusion detection systems.
- Antivirus and anti-malware software.
- Regular software updates and patch management.
- Employee cybersecurity training programs.
- Encrypted communication tools.
- Secure password policies and management.
- Other (please specify) _____

30. If any, how accessible are these tools to community members?

- Very Accessible.
- Somewhat Accessible.
- Not Accessible.

SECTION H: Deterrence (Construct)

31. In your opinion, do you believe that implementing effective cybersecurity measures can deter cybercriminals in rural communities like Mopani?

- Strongly Agree.
- Agree.
- Neutral.
- Disagree.
- Strongly Disagree.

32. What additional cybersecurity measures do you think can serve as a deterrent to cybercriminal activities in Mopani? (Select all that apply):

☐ Improved cybersecurity education and awareness programs.

☐ Strengthening local law enforcement's capacity to address cybercrime.

☐ Encouraging businesses to adopt stronger cybersecurity practices.

☐ Promoting the use of multi-factor authentication (MFA).

☐ Enhancing local cybersecurity infrastructure. o Implementing stricter penalties for cybercriminals.

☐ Fostering collaboration between local organizations and government agencies.

☐ Other (please specify) _____

ANNEXURE C: LANGUAGE EDITING LETTER

ZEE EDITING AND PROOFREADING SERVICES
PO BOX 663 THOLONGWE 0734
LANGUAGE MATTERS

05 May 2024

TO WHOM IT MAY CONCERN

This is to certify that the dissertation titled "Cybersecurity Awareness Strategy for Rural Communities: A Case Study of the Mopani District in the Limpopo Province" by Pholosho Wisani Masilane, student number 18019432 has been edited and proofread for grammar, spelling, punctuation, overall style and logical flow. The edits were carried out using the "Track changes" feature in MS Word, giving the author final control over whether to accept or reject effected changes prior to submission, provided the changes I recommended are effected to the text, the language is of an acceptable standard.

Please don't hesitate to contact me for any enquiry.

Kind regards

Prof Hlaviso Motlhaka (BEDSPF-UL, BA Hons-UL, MA-IUP: USA, PhD-WITS, PGDiP-SUN)
Cell number: 079-721-0620/078-196-4459
Email address: hlavisomhlanga@yahoo.com