BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

CHALLENGES AND BARRIERS TO REPORTING AND PROSECUTING CYBERCRIME IN BINDURA DISTRICT.

By

MAKOSA JOHN

B222403A

SUPERVISOR: MR CHITUMA F.

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELLOR OF BUSINESS AND ADMINISTRATION POLICE AND SECURITY STUDIES

2025

BINDURA

APPROVAL FORM

The undersigned certify that they have read and recommended to the Bindura University of Science Education for acceptance of the research proposal entitled "To identify the challenges and barriers to reporting and prosecuting cybercrime in Bindura district." submitted by Makosa John in partial fulfilment of the requirements for bachelor of business and administration.

Student signature........,....................

Date.......22/08/25........................

Supervisor(s) Signature...

Date........23/08/25.....................................

Chairperson Signature....... ....

11/9/25

Date...........................

RELEASE FORM

I certify that the following student MAKOSA JOHN, Student Number B222403A was under my supervision. I certify that he has attended all the scheduled meetings with me and has fulfilled all the requirements I set before him as the Supervisor. It is my professional judgment that the dissertation is of a sufficiently high standard to be submitted with my name attached to it as the Supervisor. I hereby release the student without reservation to submit his dissertation for marking.

Name of Supervisor…………………………………...

Signature………………………………………………

Date: **March 2025**

DEDICATION

This research is dedicated to my family, my unwavering pillar of strength throughout this journey. Your encouragement and support inspired me to persevere, even in the face of challenges. To my children, who have taught me the true value of education and hard work, your belief in me has been a constant source of motivation. Thank you for being my guiding light.

ABSTRACT

This study explores the challenges and barriers to reporting and prosecuting cybercrime in Bindura District, Mashonaland Central Province, Zimbabwe. As digital technology becomes increasingly integrated into daily life, the prevalence of cybercrime has risen, posing significant threats to individuals and organizations. Despite the growing incidence of these crimes, underreporting remains a critical issue, hindering effective law enforcement and prosecution. Through a mixed-methods approach, this research identifies key obstacles faced by victims, including a lack of awareness about cybercrime, insufficient legal frameworks, and limited resources within law enforcement agencies. Additionally, social stigma and fear of retaliation deter individuals from coming forward. Statistical Package for Social Science (SPSS) based descriptive statistical measures were used for quantitative data and whilst content and thematic analysis of qualitative data was done using the NVivo version 14 software for Windows and Excel. Data was presented visually in the form of tables and charts. The findings highlight the need for enhanced public education on cybercrime, improved collaboration between law enforcement and community stakeholders, and the development of robust legal mechanisms to address these challenges. This study aims to provide insights that can inform policy recommendations and strategies to strengthen the response to cybercrime in Bindura District, ultimately fostering a safer digital environment for all residents.

DECLARATION

I Makosa John registration number B222403A declare that this submission is my own work and that, to the best of my knowledge it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the reward of any other degree or diploma of the University or other institute of higher learning except where due acknowledgement has been made in the text.

Name: MAKOSA JOHN

Signature ………………………………

Date: MARCH 2025

ACKNOWLEDGEMENTS

I am profoundly grateful to the Lord God for His unwavering support throughout this project. My heartfelt thanks go to my immediate supervisor, Mr. F. Chituma, and the department chairperson, Mrs Chinyoka, for their invaluable guidance, assistance, and encouragement. Their insightful feedback and constructive criticism inspired me to reach for greater heights.

I would also like to extend my deepest appreciation to my family and siblings for their constant encouragement and steadfast support. A special thank you to all the respondents who contributed their time and insights, enabling me to gather the data necessary for this study.

Finally, I am thankful to my fellow students and colleagues for their encouragement and camaraderie during this journey. Your support has meant the world to me. May God bless you all.

ABBREVIATIONS

AI	Artificial Intelligence
APWG	Anti-Phishing Working Group
ATMs	Automated Teller Machines
BUSE	Bindura University of Science Education
FTC	Federal Trade Commission
IoT	Internet of Things
RAT	Routine Activities Theory
SCT	Self-Control Theory
SLT	Social Learning Theory
SMS	Short message service
URLs	Uniform Resource Locators
ZIMSTAT	Zimbabwe National Statistics Agency

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.0 Introduction

This chapter is an introductory section, which gives a brief background, challenges, and barriers to reporting and prosecuting cybercrime in Bindura district. The proposal aims to investigate the challenges and barriers to reporting and prosecution of cybercrime, with a specific focus on Bindura district in Zimbabwe. The study is motivated by the need to understand how cybercrimes are being reported and prosecuted, particularly a developing economy like Zimbabwe. The researcher will use questionnaires and interview guide to gather information and graphical presentations will also be made to make vivid illustrations of the concerned study. In this study, the main area of focus is to carry out a study to determine the challenges and barriers to reporting and prosecuting cybercrime in Bindura district.

1.1 Background of the Study

Cybercrime is a growing concern in Zimbabwe, with increasing reports of other digital offenses, a growing concern (Moyo, 2020). The country's economy and political instability have contributed to a rise in cybercrime as criminals take advantage of vulnerabilities in the financial and political systems. Despite efforts by law enforcement agencies, cybercrime remains a significant challenge in Zimbabwe, with many cases going unreported or unsolved. Bindura district, located in Mashonaland Central province, is a rural area with limited internet penetration and digital literacy, according to the Cybercrime report (2020) by the Zimbabwe Republic Police.

On a Global scale, cybercrime laws and definitions vary significantly across countries, making international cooperation on prosecution and reporting fragmented (Jiang, 2023). Then, the evolution of technology outpaces legal frameworks, complicating both the identification and prosecution of cybercriminals. Furthermore, global disparities in cybersecurity awareness and education contribute to vulnerabilities, especially in underdeveloped or developing regions (Zafar et al., 2022).

Locally, the existing laws in Zimbabwe may not adequately cover the wide scope of cybercrime, leading to gaps in enforcement. Efforts like the Cyber and Data Protection Bill are ongoing, but there may still be limitations in law enforcement capacity (Hartzog & Richards, 2020). Apart from that, law enforcement often lacks the necessary resources, training, and technical expertise to actively investigate cybercrime incidents. Also, a general mistrust in governmental structures may deter victims from reporting cybercrimes, fearing inadequate responses or potential victimization (Wilson et al., 2021). In addition, cultural norms, including reluctance to involve authorities in personal or family matters, can inhibit reporting.

Precisely in Bindura District, limited knowledge about the nature of cyber threats and the importance of reporting them can hinder local efforts to address cybercrime effectively (Ene & Imo, 2024). Also, variability in access to technology and the internet can create unequal opportunities for cybercriminals to exploit unsuspecting individuals or businesses. Additionally, local police forces may struggle with technological expertise and collaboration with national cybercrime units, limiting their effectiveness (Nowacki & Willits, 2020). Most importantly, initiatives to educate the community about cybercrime and promote reporting are often underfunded or poorly implemented. Victims may fear social stigma or retribution from perpetrators, leading to underreporting as well.

However, with the growth of mobile phone usage and internet access, cybercrime is becoming a concern in the district (Ene & Imo, 2024). Local individuals are vulnerable to cybercrime, particularly digital offenses. There is a need for research on cybercrime in the Bindura district to understand the problem's impact and identify effective strategies for prevention and mitigation (Sibanda et al., 2022). This background and context set the stage for a research project that aims to investigate cybercrime in the Bindura district, identify the challenges and opportunities, and provide recommendations for improving cybersecurity in the district.

Addressing the challenges and barriers to reporting and prosecuting cybercrime in the Bindura District necessitates a multi-faceted approach that considers these global, national, and local issues (Sutherland, 2004). Improving legislative frameworks, enhancing law enforcement training, promoting public awareness, and fostering community trust in reporting mechanisms are essential steps. Such efforts can help create a more responsive and resilient system to combat cybercrime effectively.

1.2 Statement of the Problem

The escalating threat of cybercrime poses severe risks to the security and well-being of individuals and communities in the Bindura District, Zimbabwe, with preliminary investigations revealing a disturbing lack of effective reporting and prosecution mechanisms. The global rise in cyber incidents, as noted by the International Telecommunication Union (ITU, 2020), has been mirrored in Zimbabwe, where cybercrime cases have surged by over 50% in the last decade. Common cybercriminal activities such as identity theft and scamming are becoming increasingly prevalent, with 65% of Zimbabweans lacking even basic cybersecurity knowledge (African Cybersecurity Report, 2020). Compounding this issue is the underfunding of Zimbabwe's cybersecurity infrastructure, with only 10% of organizations implementing adequate protection and a severe shortage of trained law enforcement officers capable of handling cybercrime cases. Bindura has seen a staggering 45% increase in cybercrime incidents, yet only 15% of victims report the crimes due to fear, mistrust in law enforcement, and a lack of awareness about reporting channels. The result is a growing digital vulnerability with profound economic implications for the district and the country. This research seeks to address these critical gaps by investigating the barriers to effective reporting and prosecution to enhance local cybersecurity awareness, education, and infrastructure to foster a safer digital environment for Bindura and Zimbabwe as a whole.

1.3 Objectives

1.3.1 Main Objective

To carry out a study to determine the challenges and barriers to reporting and prosecuting cybercrime in the Bindura district.

1.3.2 Specific Objectives

i. To determine the challenges to reporting and prosecuting cybercrime in the Bindura district.
ii. To identify the barriers to reporting and prosecuting cybercrime in the Bindura district.
iii. To describe the nature of cybercrime that takes place in the Bindura district.
iv. To recommend a cybercrime elimination guide to be used in Bindura district

1.3.3 Research Questions

i. What are the biggest challenges to reporting and prosecuting cybercrime in the Bindura district?
ii. What are the barriers to reporting and prosecuting cybercrime in the Bindura district?
iii. Does the cybercrime that takes place in Bindura district have social and economic effects on the residents and the community?
iv. What cybercrime guide can be recommended to eliminate cybercrimes in the Bindura District?

1.3.4 Significance of the Study

This study, through identifying the challenges and barriers to reporting and prosecuting cybercrime in the Bindura district, will contribute to the existing body of knowledge on cybercrime in Africa, specifically in Zimbabwe. The theoretical significance of the study on cybercrime is that it informs and extends existing theories on cybercrime. These theories are Routine Activities Theory (RAT) and Self-Control Theory (SCT). The study also provides insights into the intersection of technology, crime, and society in a developing country context. The study will also shed light on the experiences of cybercrime victims, offenders, and law enforcement agencies in the Bindura district. The study will help inform the development of effective strategies for cybercrime prevention, detection, and response in Zimbabwe and similar contexts. The study will also enhance understanding of the social, economic and cultural factors that influence cybercrime in the Bindura district. The research will also help develop a framework for understanding and addressing cybercrime in Africa. By exploring these theoretical aspects, your study can help advance the field of cybercrime research and inform evidence-based policies and practices.

1.4 Assumptions

1.4.1 Underreporting

It is often assumed that a significant portion of cybercrimes goes unreported due to various reasons, such as lack of awareness, fear of repercussions, uncertainty about the reporting process, or concerns about reputational damage.

1.4.2 Jurisdictional Issues

There is an assumption that cybercrimes are typically transnational, which can lead to challenges in determining jurisdiction, coordinating investigations across borders, This requires cooperation between law enforcement agencies in different countries.

1.4.3 Technological Complexity

It is assumed that the ever changing nature of technology presents challenges for law enforcement in understanding and investigating sophisticated cybercrimes, including those involving encryption, anonymization tools, and emerging technologies.

1.5 Delimitations of the study

1.5.1 Geographic Delimitation

Delimitations are the boundaries or limitations that are intentionally imposed on a study to focus the research and provide a clear direction. The research will be conducted in Zimbabwe, and it will focus on identifying the challenges and barriers to reporting and prosecuting cybercrime in the Bindura district. The study is limited to Bindura district, Zimbabwe, and only includes individuals and businesses in Bindura district.

1.6 Limitations

The researcher will encounter the limitations as the study progresses and will highlight them at the end of the research. Anticipated limitations such as power cuts. Questionnaires have their limitations, and these limitations include differences in understanding and interpretation, it is hard to express or pass on feelings and emotions, the respondents might be biased since they might have a hidden agenda in the issue being researched, unconscientious responses by respondents, and also accessibility issues. Differences in understanding and interpretation are limitations that can be experienced.

1.7 Definition of terms

1.7.1 Challenges

These are difficulties or obstacles that must be overcome in order to achieve a goal or task (Morrison-Smith, & Ruiz, 2020). They can arise from various sources, including external conditions, complex situations, or internal factors such as skills and resources. Challenges often require problem-solving, adaptation, and resilience to navigate successfully (Fey & Kock, 2022).

1.7.2 Barriers

These are obstacles or hindrances that prevent progress or make it difficult to achieve a goal. (Morrison-Smith & Ruiz, 2020). They can be physical, psychological, social, or systemic. Barriers may include lack of resources, inadequate infrastructure, social stigma, legal restrictions, or personal limitations that obstruct access or participation in certain activities or processes (Aguwa et al., 2023).

1.7.3 Reporting

Is the act of formally notifying authorities or relevant organizations about an event, incident, or situation, often involving the provision of detailed information (Firmin et al., 2022). In the context of crime or misconduct, reporting typically involves documenting and communicating facts about the occurrence to facilitate investigation, accountability, or action. This process can include submitting a complaint, filing a police report, or informing regulatory bodies (Syafei et al., 2024).

1.7.4 Prosecuting

This refers to the legal process of pursuing a case against an individual or entity accused of committing a crime (Billah, 2021). It involves the government or designated authority presenting evidence in a court of law to seek a conviction and impose penalties. The prosecution aims to hold the accused accountable for their actions, ensuring justice is served by the law (Bellin, 2020).

1.7.5 Cybercrime

Cybercrime refers to illegal activities conducted using computers or the internet (Shameem et al, 2022). One of the common forms is hacking. There is also online fraud and the distribution of malware. Cybercrime can target individuals, organizations, or governments, and it often involves the exploitation of technology for malicious purposes, leading to financial loss, privacy breaches, and other significant harm (Kumar, 2023).

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

This chapter aims to provide an overview of the literature and how it relates to the research study. A look at conceptual and theoretical narratives related to cybercrime and the models in place. The focus will also be on landmark models and, at the same time, look at current trends used by others and how they affect challenges and barriers to reporting and prosecuting cybercrime in the Bindura district. Further, it will explore how it affects the Bindura community and its residents socially and economically. A literature review refers to the works that the researcher read in order to elaborate on the topic and to see what has been researched previously (Iszatt-White et al., 2022). The literature review should show these two types of literature, that is, theoretical and conceptual literature, as well as empirical literature.

This literature review analyses global, regional, and local perspectives on prosecuting cybercrime, emphasizing best practices, emerging technologies, and community dynamics (Wright, 2023). The best practices were witnessed by Estonia's Cybersecurity Legislature. Estonia is currently a notable global leader in cybersecurity post-2007 cyberattacks. The nation emphasizes public-private partnerships involving citizens, businesses, and governmental agencies in cybersecurity efforts. They established a national cybersecurity strategy that includes training programs, awareness campaigns, and ongoing collaboration with international bodies for information sharing (von Solms, 2022).

Then, Singapore has integrated cybersecurity into national policy, developing a robust legal framework that includes specific cybercrime laws, a dedicated cybercrime unit within the police force, and public engagement initiatives (Alhalafi & Veeraraghavan, 2021). Regular training and exercises enhance cyber response capabilities. Additionally, the U.S. utilizes an extensive network of law enforcement agencies such as FBI and NSA to address cybercrime (Chua et al., 2022). The use of intelligence-sharing platforms and international partnerships has helped enhance investigative capabilities.

Artificial Intelligence (AI) both aids law enforcement and poses new risks. AI can detect patterns and anomalies in vast datasets, helping identify threats (Balantrapu, 2024). However, cybercriminals also leverage AI for sophisticated phishing attacks and malware deployment, necessitating adaptive security measures. In the same vein, Blockchain's decentralization offers promise for secure transactions and tamper-proof data, which can deter certain types of fraud. However, the anonymity characteristic of cryptocurrencies complicates the tracking of illicit activities (Tahira et al., 2023).

Primarily, many African nations face significant challenges, including inadequate funding for law enforcement agencies, limited access to technology, and insufficient training in cybercrime investigation skills (Paul & Iyelolu, 2024). This lack of resources hinders effective responses to cyber threats and crime. Secondly, many countries grapple with basic internet infrastructure issues, which can limit access to necessary data for investigations and impede efforts to safeguard citizens from online threats (Arshad et al., 2021).

For instance, Nigeria's Cybercrime Act (2015) serves as a model within Africa for establishing a legal basis to combat cybercrime. However, its effectiveness is hindered by enforcement issues, a lack of resources, and public distrust in law enforcement. Interestingly, Kenya has implemented initiatives like the National Cybersecurity Strategy and the National Computer Incident Response Team (CIRT) to better address cybercrime through coordinated national efforts (Arunga, 2023). Despite progress, challenges include enhancing public awareness and fostering trust.

Awareness campaigns and local initiatives, often run by NGOs and community groups, aim to raise awareness about the risks associated with cybercrime (Chang & Coppel, 2020). Programs educate communities about reporting mechanisms and digital safety practices. Partnerships with schools in cyber safety education help instill understanding from a young age, encouraging proactive behavior in online environments (Adiyono & Anshor, 2024).

Individuals from lower socioeconomic backgrounds may face barriers such as inadequate access to technology or fear of economic repercussions, influencing their willingness to report cybercrimes (Leist et al., 2021). It has also been noted that victims with fewer resources are less likely to engage with law enforcement due to perceived ineffectiveness or lack of support.

Cultural beliefs and attitudes towards technology can significantly influence how cybercrime is perceived. In some communities, there may be a stigma attached to reporting crimes committed online, leading to underreporting (Wilson, 2021). In addition, cultural factors that affect trust in law enforcement can also impact reporting behaviors. Where there is a history of negative interactions with police or distrust in governmental institutions, individuals may be hesitant to report cybercrime (Wall, 2024).

Ultimately, this literature review highlights the multi-layered nature of challenges in prosecuting cybercrime at global, regional, and local levels (Adisa, 2023). Best practices and emerging technologies from various countries illustrate effective approaches to managing cybercrime, while specific challenges faced by African nations shed light on systemic issues that need to be addressed. Furthermore, local considerations emphasize the importance of community engagement, socioeconomic status, and cultural attitudes as pivotal factors influencing both reporting and prosecution efforts (Dunlea, 2022). Addressing these dimensions holistically will be crucial in developing effective anti-cybercrime strategies tailored to the needs of specific communities.

2.1 Conceptual framework

Creating a comprehensive conceptual framework for understanding the challenges and barriers to reporting and prosecuting cybercrime in Bindura District requires a multifaceted approach. This framework should encompass global, regional, and local literature to identify existing gaps, which can inform further research or interventions. Cybercrime encompasses a range of offenses, including identity theft, cyberbullying, data breaches, and online fraud (Imoisi et al, 2021). The staggering growth in cybercrime rates and costs, influencing legislative frameworks and law enforcement practices.

In Zimbabwe, local law enforcement and reporting mechanisms for cybercrime have evolved in response to the growing prevalence of cyber-related offenses (Maluleke, 2023). This response reflects both the challenges of policing in a digital age and the strategies being implemented to enhance user safety and security. Cybersecurity and Data Protection Bill in Zimbabwe has made strides toward a more organized legal framework, with proposed legislation aimed at addressing cybercrime, data protection, and privacy concerns. The Criminal Law (Codification and Reform) Act includes provisions that can cover some aspects of cybercrime, such as fraud and harassment (Ndawana, & Chisambiro, 2024).

The Zimbabwe Republic Police (ZRP) is the main law enforcement body responsible for addressing cybercrime. The Police has specialized units, such as the Anti-Cyber Crime Unit, which focuses on investigating cyber offenses (Hilal et al, 2024). Cyber Security and Data

Protection Authority was established to oversee and implement policies related to cybersecurity as well as data protection. This agency is key in promoting awareness and providing support for law enforcement.

2.3 Reporting Mechanisms

Martin (2022) alluded that while victims of cybercrime are encouraged to report incidents at their nearest police station, the effectiveness of this process is often undermined by a significant lack of specialized knowledge and training among law enforcement officers, which can lead to underreporting and mishandling of cases. Although initiatives such as hotlines and online reporting platforms have been introduced to improve accessibility, their impact is frequently diluted by inconsistent public awareness and variable effectiveness (Faik et al, 2024). Furthermore, while local NGOs and government bodies play a critical role in raising awareness through community campaigns, these efforts are often fragmented and insufficient to foster widespread understanding of the complexities of cybercrime, leaving many individuals ill-equipped to protect themselves or seek justice. Without a cohesive, well-informed approach, these mechanisms risk falling short in the fight against the growing threat of cybercrime (Piacquadio, 2024).

2.4 Challenges Faced in Effectively Investigating and Prosecuting Cybercrimes

Law enforcement agencies often struggle with inadequate resources and training, which affects their ability to effectively investigate and prosecute cybercrimes (McKoy, 2021). Additionally, there is generally low public awareness about what constitutes cybercrime and how to report it, which leads to underreporting. Apart from that, insufficient technological infrastructure and tools within law enforcement agencies hinder effective responses to cyber incidents (Sarkar & Shukla, 2023). In addition, the perceived inefficacy of law enforcement and fear of victim-blaming can deter citizens from reporting.

To improve local law enforcement and reporting mechanisms in Zimbabwe, there is a need to enhance training. Offering specialized training to law enforcement on cybercrime investigation and forensic techniques. Then also creates user-friendly reporting systems by developing more accessible and user-friendly online reporting platforms for cybercrime (Maingi, 2022). More importantly, launching comprehensive awareness campaigns emphasizing the importance of reporting and the protections available to victims. It would also be helpful to ensure that local law enforcement is adequately funded and equipped to deal with the complexities of cyber offenses (Monaghan, 2020).

All in all, while Zimbabwe has made progress in establishing law enforcement structures to combat cybercrime, significant challenges remain. Enhancing these mechanisms through better training, resources, and public engagement will be critical for effective cybercrime management (Sarkar & Shukla, 2023).

2.5 Community Initiatives

NGOs frequently partner with police to conduct training and awareness programs to promote better understanding and engagement in cybercrime reporting (Chang & Coppel, 2020). Also, schools and community centers may facilitate educational sessions on digital safety and cybersecurity to empower citizens.

2.6 Legal Framework

The Cybersecurity and Data Protection Bill aims to profer legal framework for cybersecurity and data protection (Raul, 2021). The bill is still pending full enactment, which can create gaps in immediate prosecutorial power. The Criminal Law (Codification and Reform) Act contains provisions that can be applied to various offenses related to cybercrime, including fraud and harassment. However, its coverage is limited and often does not address modern digital offenses specifically.

The Proposed Electronic Transactions and Cyberspace Bill has been proposed to address issues related to electronic transactions, but again, full implementation has yet to be achieved (Sulastri & Cartin-Pecson, 2024). Existing laws sometimes fail to clearly define cybercrime, leading to difficulties in prosecution. For instance, terms related to “computer crimes” or “data breaches” might lack specificity in legal contexts. The lack of a centralized legal framework or a clear strategy for enforcing cyber laws can result in inconsistent application and difficulty for prosecutors in navigating legal processes (AllahRakha, 2024). Similarly, citizens may be unaware of what constitutes cybercrime, hindering their ability to report offenses. Moreover, misconceptions about the law can also affect how cases are pursued.

2.7 Training and Skill Development

Law enforcement agencies often lack the technology needed to effectively investigate and prosecute cybercrimes (Chua et al, 2022). This includes forensic software, secure data storage, and appropriate hardware. Also, limited budgets affect the ability of agencies to acquire necessary technology, conduct training, or even hire specialized personnel (Napathorn, 2022).

Many local law enforcement officers may not have received adequate training in digital forensics, the technical aspects of cybercrime, or how to gather evidence from electronic devices (Martin, 2021). Training programs that focus on cyber investigations are essential; however, they may be infrequent or non-existent. Collaboration with international cybersecurity and law enforcement organizations can help build local capacity. Effective prosecution often requires coordination with multiple law enforcement agencies (national and international), and specialized training in collaborative processes is limited (Dallier et al, 2021).

2.8 Jurisdiction Issues

Cybercrime often transcends borders, making prosecution complicated. For example, if a crime is committed online in Zimbabwe but the perpetrator resides in another country, pursuing prosecution may require complex legal negotiations. In addition, Zimbabwe's engagement in international legal treaties such as the Budapest Convention on Cybercrime (Malunga, 2022). Without these agreements, pursuing cases across jurisdictions becomes exceptionally challenging.

Also, variations in laws across different countries can result in situations where an action deemed illegal in Zimbabwe may not be considered a crime in another jurisdiction (Malunga, 2022). This complicates collaboration and complicates extradition requests. Apart from that, gathering digital evidence often involves navigating through different national laws regarding data privacy, which can create barriers to accessing necessary information (Fabbrini & Celeste, 2020). The differences in judicial processes and protocols can significantly impact case progression.

Possibly, the challenges associated with the prosecution of cybercrime in Zimbabwe are multi-faceted, involving limitations in legal frameworks, resource constraints, and complexities in jurisdiction (Taruvinga, 2020). Addressing these issues requires a comprehensive approach, including updating and harmonizing laws, enhancing technological capacity and training within law enforcement, and fostering international cooperation for effective cybercrime prosecution. Collaborative efforts among governmental bodies, NGOs, and international partners will be crucial in creating a more resilient and effective legal and investigative framework for combating cybercrime (Świątkowska, 2020).

2.9 Training and Capacity Building

Law enforcement officials often lack specialized training in cybercrime investigation techniques, digital forensics, and the technical aspects of data retrieval (Sharma, 2024). Without this skill set, they may be ill-equipped to handle sophisticated cyber offenses. More so, many countries have established cybercrime units, but without ongoing training and professional development, these units can lose effectiveness (Whelan & Harkin, 2021). Continuous education on emerging threats and evolving technologies is necessary.

Collaborations with international law enforcement bodies and cybersecurity organizations can provide local agencies with better training resources and expertise (AllahRakha, 2024). Also providing law enforcement with access to the latest tools and technologies for investigation, such as forensic software and data analysis tools, can significantly enhance their capacity to tackle cybercrime effectively.

2.10 Community Relations

Historical mistrust and negative relationships between communities and law enforcement often result in communities being hesitant to report cybercrimes (McKoy, 2021). This reluctance is compounded by the fear of victim-blaming or ineffectiveness in responses. Additionally, police forces need to actively engage with community members through outreach programs, public forums, and trust-building initiatives aimed at fostering cooperation in reporting and preventing cybercrime.

Law enforcement agencies must communicate openly about how reports are handled and the outcomes of investigations (Jennings & Perez, 2020). Prospective transparency can help build community confidence in law enforcement’s effectiveness. As well as implementing feedback systems where community members can express their concerns regarding policing strategies related to cybercrime can assist in tailoring approaches that resonate better with community needs (Sarkar & Shukla, 2023).

2.11 Legislative Framework

Many existing laws frame cybercrime in outdated contexts, lacking the ability to address new threats such as ransomware, data breaches, and digital scams effectively (Smith, 2024). Furthermore, current laws may cover only specific types of offenses or fail to consider the cross-border nature of cybercrime. Comprehensive legislation should address various offenses, outline penalties, and specify investigative procedures for law enforcement.

Strong data protection laws are critical, not only to safeguard citizens' information but also to provide law enforcement with clear guidelines for collecting and processing data during investigations (Doe, 2024). Moreover, engagement with international legal frameworks, such as the Budapest Convention, can help unify efforts to combat cybercrime across borders and enable better cooperation among nations in prosecuting cybercriminals.

To this end, developing a conceptual framework to address the challenges of reporting and prosecuting cybercrime in Bindura District involves a layered understanding of technology, legal frameworks, community engagement, and resource allocation. By synthesizing literature at local, regional, and global levels, researchers can identify key gaps and formulate targeted interventions that encourage a more robust response to cybercrime threats (Wright, 2023). Addressing these gaps will require a concerted effort from governments, law enforcement agencies, community organizations, and citizens.

2.12 Theoretical framework

The theoretical framework for identifying the challenges and barriers to reporting and prosecuting cybercrime integrates various criminological theories and concepts. This multi-theoretical approach helps to unpack the complexities surrounding cybercrime and the systemic issues that hinder effective reporting and prosecution (Rapisarda & Kras, 2023).

2.12.1 Routine Activity Theory (RAT)

RAT is a criminology theory that was first proposed by Lawrence E. Cohen and Marcus Felson in 1979. It posits that crimes tend to occur multiple triggering elements converge. These are time and opportunity, a motivated offender, an acquirable target, and the absence of safeguards. The theory explains how cybercrime opportunities arise from the merging of factors such as motivated offenders, available targets, and the absence of capable guardians (Govender et al., 2021). According to Routine Activity Theory, crime is more likely to occur when these elements converge. The theory also emphasises that alterations in routine activities and lifestyle patterns can influence the likelihood of criminal activity. As an example, changes in technology, shifts in social norms, or alterations in the physical environment can affect the occurrence of crime (Miró-Llinares & Moneva, 2020).

Routine Activity Theory has been applied to various types of crime such as property crimes, theft, vandalism and interpersonal violence (Nazaretian & Fitch, 2021). It has implications for crime prevention strategies. It suggests that efforts to reduce crime should focus on deterring the multiple factors from converging. Calder et al., (2021) argued that analysing dynamics of routine activities and how they intersect with the presence or absence of key elements that facilitate crime can help policymakers, law enforcement agencies, and communities to develop more effective strategies to prevent and reduce criminal activities.

Motivated offender refers to individuals who are inclined to commit crimes. These offenders are motivated by a variety of factors such as financial gain, personal gratification, or other abstract reasons (Koegl, & Farrington, 2022). Then a suitable target is an object or individual that is attractive to the offender. Targets can vary widely and may include individuals, properties, or assets that are perceived as valuable or easy to exploit.

Finally, a capable guardian is someone or something that can prevent or deter crime from occurring. This can be a person, such as law enforcement, security personnel, or a vigilant neighbour, or it can be security measures like alarms, locks, or surveillance systems.

2.12.2 Social Learning Theory (SLT)

The theory suggests that individuals learn cybercriminal behaviour by observing and imitating others (Dearden & Parti, 2021). It is a psychological theory that suggests that people learn new behaviours through observational learning of the social behaviours of others at large. Introduced by Albert Bandura in the 1970s, this theory emphasises the how social interactions, imitation, and modelling contributes to the development of criminal behaviour. Largely, social learning theory provides valuable insights into how individuals acquire new behaviours through observation, modelling, and cognitive processes (Rumjaun & Narod, 2020). The theory explains the mechanisms of observational learning and the factors that influence imitation. Therefore, educators, psychologists, and policymakers can develop strategies to promote positive behaviours, facilitate skill acquisition, and deter negative behaviours in individuals and communities.

2.12.2.1 Concepts of Social Learning Theory

The main idea of Social Learning Theory is that individuals can learn new behaviours by observing others. Through this observational learning process, individuals can acquire new skills, attitudes, and behaviours without direct reinforcement (Rumjaun & Narod, 2020). Then, modelling involves imitating the behaviours of role models or individuals in one's social environment. People are more likely to imitate behaviours they observe if the model is perceived as credible, attractive, or having high status.

The Social Learning Theory also highlights the role of vicarious reinforcement and observing the consequences of others' actions and adjusting one's behaviour based on these observations. In addition, the theory emphasises the importance of cognitive functions in learning (Rumjaun & Narod, 2020). Individuals actively process information about observed behaviours, make judgments about the likely outcomes of those behaviours, and decide whether to imitate them based on their assessments. This is self-efficacy. This is defined as an individual's belief that they can perform a specific task or behaviour (Schunk & DiBenedetto, 2022). Self-efficacy therefore plays a role in motivating behaviour and influences people to imitate others.

The theory has been used in various disciplines such as education, psychology, and criminology. In education, it has implications for teaching methods that promote observational learning and positive modelling. In psychology, it is used to understand behaviour change and therapy (Sellers et al., 2020). In criminology, it helps explain how individuals learn criminal behaviours through observation and imitation.

2.12.3 Strain Theory

Strain Theory argues that societal pressures can motivate individuals to commit crimes. This is applicable in situations where they feel unable to achieve socially accepted goals through legitimate means (Nickerson, 2023). In the digital context, individuals may resort to cybercrime due to economic pressures, unemployment, or social marginalization. This theory highlights how socio-economic factors drive individuals toward cybercrime. It emphasises the importance of creating supportive systems that provide legitimate opportunities for success.

2.12.4 Deterrence Theory

According to McGarry (2021) the theory suggests that the threat of punishment can deter potential criminals or individuals from committing crime. The assumption is that individuals weigh the potential benefits or implications of committing a crime before engaging in criminal behaviour. Therefore, the perceived risk of punishment serves as a deterrent to prevent criminal acts (Sellers et al., 2020). While deterrence theory remains a foundational concept in criminology and criminal justice, researchers continue to investigate its complexities and nuances to improve our understanding of how punishment, risk perception, and other factors influence criminal behaviour and the effectiveness of deterrence strategies.

2.12.4.1 Contents of Deterrence Theory

General deterrence aims to prevent crime by making examples of offenders through punishment. The assumption is that the fear of punishment deters potential offenders from committing crimes to avoid the negative consequences associated with law-breaking (Uzoka & Nwabachili, 2023). Specific deterrence targets individuals who have already engaged in criminal behaviour and tries to hinder them from repeating offenses. This is done through imposing sanctions or punishments on offenders to discourage them from committing future crimes.

Deterrence theory suggests that the effectiveness of deterrence is influenced by three key factors. The first one is certainty. This is the likelihood of being caught and punished for a crime (Bates & Anderson, 2021). Severity is the perceived harshness of the punishment that would be imposed if caught, and Celerity is the swiftness of the punishment following the commission of a crime. Deterrence theory has influenced policies and practices in the criminal justice system. Strategies such as increasing police presence, enhancing surveillance, implementing mandatory minimum sentences, and imposing harsh penalties for specific crimes are all rooted in the principles of deterrence theory (Smit, 2007).

2.12.4.2 Criticism and Limitations

Deterrence theory has faced criticism and limitations. Some research imply that the possibility of punishment is more influential in deterring crime than the severity of punishment (Weatherburn, 2020). Additionally, factors such as individual differences in risk-taking behaviour, social influences, and situational contexts can impact the effectiveness of deterrence strategies. Dearden& Gottschalk (2024) alluded that contemporary studies on deterrence theory have explored its application in cybercrime, white-collar crime, and terrorism. The theory is also being examined in the context of rehabilitation, restorative justice, and alternative approaches to crime prevention.

2.13 Impact of Cybercrime on Businesses

The "Impact of Cybercrime on Businesses" by Ponemon Institute (2019) reports on the financial and reputational costs of cybercrime for businesses. The Ponemon Institute is known for its research on information security, privacy, and data protection. The report provides valuable data and analysis for various stakeholders in understanding the financial, operational, and reputational consequences of cybercrime on organizations.

2.14 Empirical Literature

Empirical literature refers to past studies related to the research. It shows how these studies relate or differ from the current study, thus establishing the knowledge gap (Sampson et al., 2022). The gap may be in terms of differences in approaches, theoretical starting points. There might also be untested theories or other variables such as inadequate evidence. These are all discussed in the empirical literature review.

Knowledge of past research enables one to explore the study more comprehensively. For example, Rambanepasi (1989), Green (1993), and Mupfurutsa (1999) made various discoveries regarding the topic in question. Pandadyira and Hwinayi (2000) highlight that a good empirical literature review adds substance to the study.

Research that lacks a connection to the established body of knowledge typically has minimal impact on its field. Such studies often result in fragmented information that holds limited practical value. Engaging in a review of related literature enables researchers to refine their research questions and narrow down their study focus while providing clarity in defining essential concepts (Stewart, 2020). A thorough literature review aids in refining initial research inquiries, ensuring they are suitable for investigation. Additionally, it facilitates the precise articulation of study concepts by transforming them into measurable definitions.

According to Alyahyan & Düştegör (2020), conducting an effective literature review frequently contributes to the development of hypotheses regarding variable relationships in a study. Research that includes hypothesis testing generally offers more substantial contributions compared to studies lacking hypotheses or structured research questions.

A critical examination of relevant literature frequently provides insight into discrepancies in research findings (Ali, 2022). Variations or contradictions in study results may stem from differences in research design, the types of instruments utilized, or the methodologies and analytical approaches applied. By comparing the procedures employed in various studies, researchers can identify factors contributing to inconsistencies in findings.

An extensive review of previous research enhances an understanding of which methodologies yield promising results and which approaches may be less effective (de Bruin et al., 2020). Examining related literature helps prevent unintentional duplication of past studies. Additionally, familiarizing oneself with existing theories and prior research fosters a deeper comprehension of how new findings integrate into the broader academic framework (Dunne & Ustundag, 2020). At this stage, it is essential for researchers to explore empirical studies directly relevant to their area of inquiry.Cybercrime and the Internet by David Wall (2001) explores the emergence of cybercrime and its relationship with the Internet. It is a notable book that delves into the realm of cybercrime and its relationship with the internet. David Wall, a prominent scholar in the field of criminology, provides insights on cybercrime and the challenges posed by the internet as a platform for criminal activities. The book is insightful for researchers, policymakers, law enforcement professionals and individuals interested in understanding the complex interplay between technology, crime, and society in the digital age (Wilson, 2020).

This theoretical framework provides a lens for examining the challenges and barriers to reporting and prosecuting cybercrime in Bindura. By integrating diverse theories, it highlights the multifaceted nature of cybercrime and the systemic issues that hinder effective responses (AllahRakha, 2024). The suggestion is that addressing these challenges requires a collaborative approach that encompasses education, policy reform, and enhanced support for victims, ultimately fostering a safer digital environment locally and beyond the borders at large.

2.15 Research Gap

Despite the increasing prevalence of cybercrime globally, there is a notable gap in the literature specifically addressing the challenges and barriers to reporting and prosecuting cybercrime within the context of Bindura District, Zimbabwe. While studies have examined cybercrime in broader national and international contexts, such as the work of Wall (2007) and Yar (2005), these analyses often overlook localized factors that influence reporting behaviors and prosecutorial effectiveness in specific regions.

Existing research highlights various barriers to reporting cybercrime, including victim reluctance due to fear of stigma and lack of trust in law enforcement (Holt & Bossler, 2016; McGuire & Dowling, 2021). However, there is a shortage of empirical studies that focus on the unique socio-economic and cultural dynamics of Bindura District, which may significantly impact individuals' willingness to report cybercrimes. For instance, the influence of local community norms, economic conditions, and the availability of technological resources has not been adequately explored in the context of Zimbabwean society.

Furthermore, while some literature discusses the inadequacies of legal frameworks in addressing cybercrime (Brenner, 2019; Kshetri, 2021), there is limited research on how these inadequacies manifest specifically in Bindura District. The lack of localized data on law enforcement capabilities, training, and resource allocation further complicates the understanding of prosecutorial challenges in this area.

To this end, the existing body of literature fails to provide adequate understanding of the specific barriers to reporting and prosecuting cybercrime in Bindura District. This research aims to fill this gap by investigating the unique challenges faced by victims and law enforcement in this region. This will contribute to a more nuanced understanding of cybercrime dynamics in Zimbabwe.

2.16 Gaps in Cybercrime Management and Prosecution

Effective management and prosecution of cybercrime require addressing several critical gaps in literacy, training, community relations, and legislative frameworks (Ene & Imo, 2024). Firstly, many individuals lack basic knowledge about what constitutes cybercrime, making them vulnerable targets. Common offenses, such as phishing, identity theft and online fraud are sometimes not recognized as crimes by the public. In the same vein, many potential victims are unaware of the proper procedures for reporting cybercrime incidents, leading to underreporting and a lack of data that could inform better policing strategies (Jimenez et al, 2024).

Secondly, there is a significant need for community-specific educational programs on digital literacy that inform the public about cyber risks. Initiatives could include workshops, seminars, and school-based programs that cover both preventive measures and reporting mechanisms (Tofa et al, 2020). The role of NGOs and Local Organizations plays a vital role in disseminating information, but their reach and resources may be limited. Collaborating with these organizations can help expand outreach efforts.

2.17 Summary

Few or fewer studies specifically target Bindura District as far as cybercrime is concerned, as most research tends to generalize findings to wider regions or countries, creating a gap in localized insights. This chapter mainly focused on providing an overview of the literature and how it relates to the research study. It also focused on the analysis of reviewed literature on the challenges and barriers to reporting and prosecuting cybercrime in Bindura district. The next chapter is the research methodology.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

The researcher seeks to have a methodological plan and map of for soliciting enough evidence to address the research questions. The methodology comprises of various elements such as a research design, population and sampling techniques and data collection procedures. Data analysis will also be handled.

3.1 Research Design

Research design is defined as the strategy that a researcher devises to combine different parts of a study in a coherent way (Allibang, 2020). It outlines the structure of the research process. It details how data will be collected, analysed, and interpreted to address the research objectives effectively. A well-thought-out research design helps enhance the validity, reliability, and generalizability of the study.

According to Creswell (2024), research designs are universally used in qualitative, quantitative, and mixed methods approaches. They can also be referred to as strategies of inquiry (Denzin & Lincoln, 2021). Salkind (2020) defines research as the act of planning and conducting research. Furthermore, Leavy (2017) looks at research design as a process of structuring a research project. These research designs have increased over time, as highlighted by Creswell (2024), because of advanced computer technology. Furthermore, the ability to analyse complex data has increased. Researcher now have the ability to use new procedures for conducting social science research (Creswell, 2024). These research designs are divided into three: quantitative, qualitative, and mixed methods.

Leavy (2017) asserts that qualitative research is characterised by inductive approaches to generate meaning through various contexts. Quantitative research is also an approach for testing theories by examining the relationship among variables. These variables, in turn, can be measured typically on instruments, so that numerical data can be analysed using statistical procedures (Creswell 2014). In addition, Creswell (2014) highlights mixed methods research combines both quantitative and qualitative data.

3.2 Mixed-methods Research

The research was carried out using mixed-methods research. Mixed-methods research is defined as an approach to inquiry that combines elements of qualitative and quantitative research methods (Giri et al., 2021). Integrating both qualitative and quantitative techniques helps provide a more nuanced comprehension of a research problem. Largely, mixed-methods research offers a flexible and comprehensive approach to inquiry that leverages the strengths of both methods to generate rich, contextualized, and robust findings that address complex research questions and contribute to an enhanced understanding of various phenomena (Sumner et al., 2023).

A mixed method study was chosen as the design in order to enable an in-depth exploration and understanding. Wisdom and Creswell (2022) stipulate that the basic assumption of this methodology is that such combining them creates a more complete and synergistic utilization of data. FoodRisc (2016) adds that one major advantage of conducting mixed methods research is the possibility of triangulation. This will help the researcher to address aspects of the phenomenon more precisely by approaching it from various vantage points using different methods and techniques (Tzagkarakis & Kritas, 2023).

This research design allows for a comprehensive exploration of cybercrime in Bindura district. The survey provides a broad overview of cybercrime experiences and perceptions, while the interviews offer insights into the perspectives of key stakeholders.

3.2.1 Justification and Merits of choosing the Mixed Method Research

Selecting mixed-methods research offers various advantages. Several justifications can be offered based on the nature of the research question, the complexity of the phenomenon being studied, and the aim of achieving a comprehensive understanding through the integration of qualitative and quantitative methods (Giri et al, 2021). The study aims to leverage the complementary strengths of qualitative and quantitative methods to address the research question effectively, explore the complexity of the phenomenon, and generate comprehensive and robust findings that contribute meaningfully to the existing body of knowledge. Cook et al., (2020) asserts that mixed-methods research has the ability to provide a more nuanced, and valid understanding of research questions and phenomena by leveraging the strengths of both qualitative and quantitative methods.

3.3 Study Population and Population Sample

Majid (2018) points out that the research population is a sample from the population of interest. According to Umar et al., (2015), a population is a specified aggregation of survey elements. In addition, Madugu et al., (2015) see a population as being made up of all conceivable subjects relating to the phenomenon of the study. Said et al., (2015) further highlight that elements and subjects refer to individual items or variables that are included in population. Under this research, the population comprises of banks, police, and residents. Data is going to be collected from the Bindura area from law enforcement officials, cybercrime victims, and community leaders.

3.4 Study Site

As in most African countries, Zimbabwe is an important repository of cybercrime. The data are going to be collected in the Bindura area. The Bindura area is the hometown of the researcher; as such, it is easy for the researcher to access the data. Bindura district is located in the Mashonaland Central Province in Zimbabwe. Bindura (Latitude: 17.3245 0 S; Longitude: 31.3330 0 E) is in Mashonaland Central province, under Natural Agro-ecological Zone 2b. It has an altitude of 1110 meters above sea level, situated 86.9 km from Harare.

3.5 Sampling Techniques

Purposive sampling based on expertise, experience, and willingness to participate. Due to the qualitative approach used by the researcher to research challenges and barriers to reporting and prosecuting cybercrime in Bindura district, the researcher used the non-probability sampling technique, which is also known as the non-random sampling technique, and also used the purposive sampling approach. Taherdoost (2016) points out that non-probability sampling is often associated with case study research design and qualitative research. Such sampling techniques dictate that a sample of participants or cases does not need to be representative. For this reason, the researcher used his discretion and knowledge in the area in selecting the major respondents.

3.6 Sampling Procedure

3.6.1 Sampling Frame

The sampling frame facilitated the identification of potential participants from the target population, including individuals, businesses, law enforcement agencies, and community leaders within Bindura District. Di-Gaetanano (2013) describes a sampling frame as a structured list of units from which a sample is selected. Similarly, Cruz-Cunha & Moreira (2011) define a sampling frame as a compilation of units that collectively represent the entire survey population. When available, this frame serves as the basis for selecting a sample. Mujere (2017) characterizes sampling as the method used to choose a suitable subset from a larger population, ensuring that the selected sample accurately reflects the characteristics and parameters of the broader group. Majid (2018) further emphasizes that sampling plays a crucial role in research, as the total population of interest is often too vast for comprehensive inclusion in a study. Consequently, selecting a representative sample becomes essential for generating reliable insights. Mujere (2016) defines a sample as a selected subset of individuals, objects, or items taken from a larger population for measurement and analysis. For this study, the sample will be drawn from Bindura District, encompassing law enforcement officials, cybercrime victims, and community leaders.

3.6.2 Sample size

The quantitative sample size will be established through sample size tables or computed using Yamane's formula for sample size determination. For qualitative sampling, theoretical sampling principles will be applied to define appropriate sample sizes (Guest et al., 2017; Saunders & Townsend, 2018). Sample size refers to the total number of observations or data points gathered within a study (Taherdoost, 2021). Rahman (2023) further defines sample size as the total number of subjects selected for a given study. This subset is drawn from the broader population and is intended to be representative of the larger group relevant to the research. A well-calculated sample size enhances the validity of the findings by ensuring they accurately reflect the entire population, minimizing potential bias while optimizing precision (Gunathilake et al., 2024). Additionally, the researcher has utilized scholarly references and established industry standards to guide and justify the sample size selection, reinforcing the methodological rigor of the study.

Sample Size Formula = [z2 * p(1-p)] / e2 / 1 + [z2 * p(1-p)] / e2 * N]

Were,

N is the population size

z is the z-score

e is the margin of error

p is the standard deviation

3.7 Research Instruments

3.7.1 Questionnaire

Researchers employ various techniques to gather data in a study. Alshengeeti (2014) emphasizes that research methods are fundamental to the success, validity, and reliability of any research project. In this study, the researcher utilized questionnaires and interviews to collect data. The primary data gathered will consist of interview insights and raw responses from participants. All data collection in this study relies on subjective judgments (Lim, 2024). A key implication of subjective data is that respondents' perspectives can vary significantly and, in some cases, contradict one another. Such discrepancies may stem not only from differences in individual knowledge but also from the contextual conditions under which responses are provided. Given these variations, incorporating multiple sources of evidence ensures a more comprehensive and reliable investigation. Jackson (2011) argues that rigid adherence to a single data collection method can restrict the scope of field research, likening it to being confined within a restrictive framework. Consequently, employing multiple data collection methods enhances the credibility of the information obtained, as different approaches complement one another, leading to findings that are both more precise and reliable.

3.7.2 Interview

According to Denscombe (2019), interviews are helpful in the collection of in-depth information from respondents. This is a qualitative research technique through an interchange of information. Also, Chinorumba (2013) says an interview is an oral questioning or two-way conversation initiated by the interviewer for the specific aim or objective of obtaining problem-related data and to gain knowledge about ideas, attitudes, opinions, and perceptions of the interviewee.

A list of questions will be drawn up, which will have both open-ended and closed-ended questions. Semi –structured interview guides (Kvale, 1996) were created to will be created to allow reflection on the part of interviewees.

3.8 Validity and Reliability

Cowburn, Gelsthorpe, and Wahidin (2017) describe ethics as a broad concept encompassing various approaches to understanding and analyzing moral life, focusing on principles of appropriate and just conduct. Komic, Marusic, and Marusic (2015) define research ethics as the examination of research practices through the lens of moral principles. Expanding on this perspective, Cowburn, Gelsthorpe, and Wahidin (2017) emphasize that ethical research must adhere to established standards, which involve safeguarding the dignity, rights, safety, and overall well-being of participants. Miller et al. (2012) further highlight that ethical considerations were historically viewed as constraints on researchers' actions in their quest for knowledge. However, contemporary perspectives regard ethics as the foundation of research itself, positioning it as a mechanism for advancing social justice. In alignment with this ethical framework, the researcher in this study will ensure adherence to ethical principles, particularly in maintaining the confidentiality and privacy of individuals and organizations involved in the research process (Green-Eneix et al., 2021).

It is of very much importance that during the investigation and data gathering of this research, the interviewees are truthfully and well advised of the aim, purpose, and the type of research being carried out (Sukmawati, 2023). This will enable them to decide whether to participate or not in the interview. Also, the researcher should advise the interviewee of the right to answer or reject if they do not feel comfortable. In addition to the above, the interviewees should also be told that all information they provide will be treated with confidentiality and applied within an academic framework (Teeger et al, 2022). Lastly, the researcher should ensure that all translations done do not contain any misinterpretation.

3.9 Pilot Test- stating

According to Thabane, Ma & Chu (2010), a pilot study is an investigation designed to test the feasibility of methods and procedures for later use on a large scale or to search for possible effects and associations that may be worth following up in a subsequent larger study. In (2017), highlighted that a pilot study is the first step of the entire research protocol and is often a smaller-sized study assisting in planning and modification of the main study. Furthermore In (2017), points out that a pilot study is performed reflecting all the procedures of the main study and validates the feasibility of the study by assessing the inclusion and exclusion criteria of the participants, preparation of the drugs and intervention, storage and testing of the instruments used for measurements in the study as well as training of researchers and research assistants. It seeks answers to find out whether something can be done, that is, should the researchers go ahead with the research, and if so, how.

The pilot study will take place in the Bindura district. Questionnaires will be issued to the law enforcement agencies and community leaders. Semi-structured interviews will be done with those law enforcement agencies.

3.10 Methods of Data Collection

3.10.1 Data Collection

Quantitative: Online survey using a questionnaire (Google Forms or Survey Monkey) administered to a random sample of 300 individuals in Bindura district. According to Abawi (2014), a questionnaire is data collection too that comprises of survey questions to be filled by respondents. In this research, both open-ended and closed-question approaches will be used on the questionnaires. This approach will purposely be used by the researcher in an attempt to maximise the results of this research method. Abawi (2014) also points out that questionnaires facilitate the collection of subjective and objective data in a large sample.

Though the researcher chose this data collection method it is also has limitations. O'Leary (2014), offers some concerns in using questionnaire as a research tool as they are time consuming, expensive and sampling is difficult. Furthermore O'Leary (2014), asserts that questionnaires are notoriously difficult to get right and they often do not go as planned.

3.11 Data Analysis

Quantitative analysis in this study involved descriptive statistics, frequency analysis, and inferential statistical techniques such as chi-square tests, ANOVA, and correlation analysis, all conducted using SPSS software. Harding and Whitehead (2013) described qualitative data analysis as the process of interpreting collected information to establish order, extract meaning, and present findings coherently. For qualitative data, NVivo software was employed to facilitate the extraction of responses relevant to the research questions. Additionally, findings were presented and analyzed using prose writing, charts, and graphs to systematically display data obtained from interviews and questionnaires (Sakakibara et al., 2021). Questionnaire data was organized within a structured grid, visually consolidating responses. Data underwent coding and analysis using appropriate scaling methods before being entered into the grid. The proportion of respondents was quantified through calculations of averages and standard deviations to ensure precise statistical representation.

3.12 Ethical Considerations

Throughout the study, the researcher prioritized the safety of participants, ensuring protection from both physical and emotional harm. Informed consent was emphasized alongside the principle of voluntary participation, which is crucial in ethical research. The researcher made it clear that participation was entirely optional, with no coercion involved. To uphold confidentiality, respondents were identified by their first and last names and the researcher assured them that all information provided would be treated with strict confidentiality and not shared with any external parties, as stated in both introductory letters and verbally. It was also clarified that the data collected would only be used for the study's purposes and that the survey results would be presented and analysed in aggregate form.

3.13 Summary

This chapter focuses on the research design, mixed-methods research, justification and merits of choosing the mixed, practical implications and complexity of the research problem. This chapter also elaborates on the population as sampling as well as validity and reliability, pilot test, sample collection, methods of data collection, data analysis. All numeric data will be analysed using NVIVO, Excel, and SPSS, and output will be shown in the appendix. Questionnaire, interview guide and pictorial results will also be shown in the appendix.

CHAPTER IV

DATA PRESENTATION, INTERPRETATION, AND DISCUSSION

4.0 Introduction

This is the chapter in which data collected from the research tasks are presented. Data analysis, interpretations, and presentations are the focus of this chapter. The Statistical Package for Social Sciences (SPSSV.23.0), Nvivo 14, and Excel were used to analyse data. The researcher used statistical software to analyse the quantitative data collected through questionnaires and presented the results in tables and figures. Additionally, the researcher utilized NVivo 14 to analyse the qualitative data obtained from open-ended questions in the questionnaires.

4.1 Response Rate

Table 1.1

The Percentage Response rate for questionnaires

Instrument	**Questionnaires Distributed/Planned**	**Questionnaires Returned/Completed**	**Percentage Response**
Questionnaires	25	20	80%

The researchers collected data from 25 individuals using questionnaires, but only 20 of the completed questionnaires were usable for analysis, resulting in an 80% response rate. Then five questionnaires were delivered online and never got a response. This may maybe because some of these participants are facing internet challenges. The response rate is on the high side, The high response rate for this study also confirms what Bless et al. (2019) showed that, reliable data collection instruments should have at least a response rate of between 20 and 40 percent.

4.2 Demographic Data

This section provides an analysis of demographic information for quantitative data relating to participants to establish the gender, age, marital status, career history, academic level, qualification of the respondents, and work experience.

4.2.1 Gender of the Respondents

When researching on challenges and barriers to reporting and prosecuting cybercrime in Bindura district, the gender of the respondents was considered and is an essential variable.

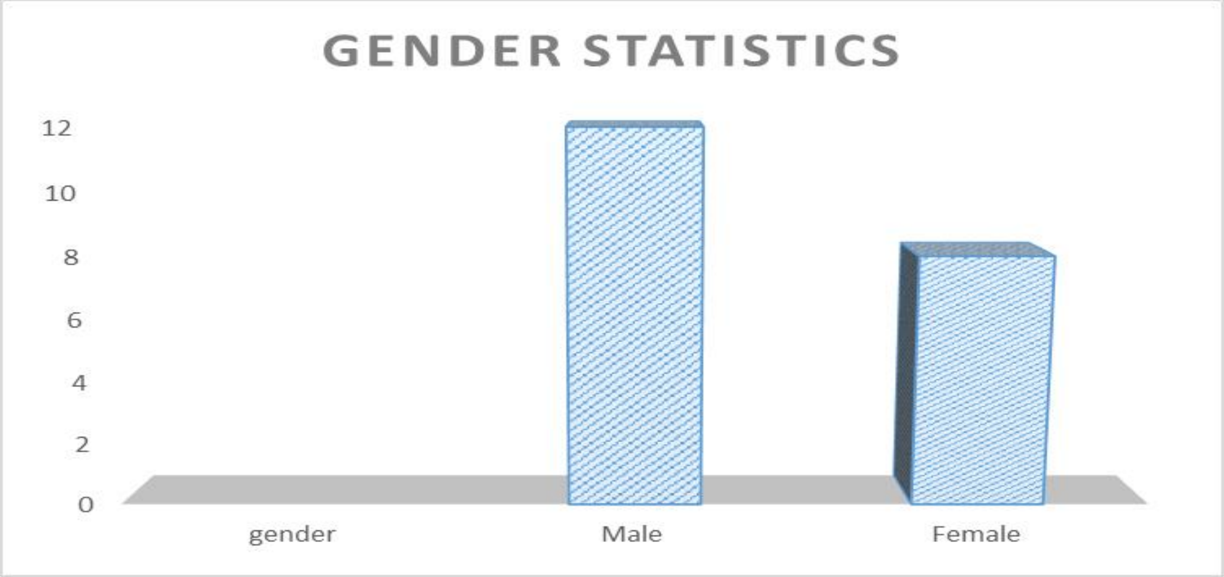

Fig 1 Gender of the Respondents

According to Figure 1, there were a total of 20 valid responses, with 12 respondents (60.0%) identifying as male and 8 respondents (40.0%) as female. The data clearly shows a notable male predominance in the sample population.

4.2.2 Age of the Respondents

The age categories of the participants in this study are diverse. Fig 2 shows the summary percentages of the respondents' age groups.

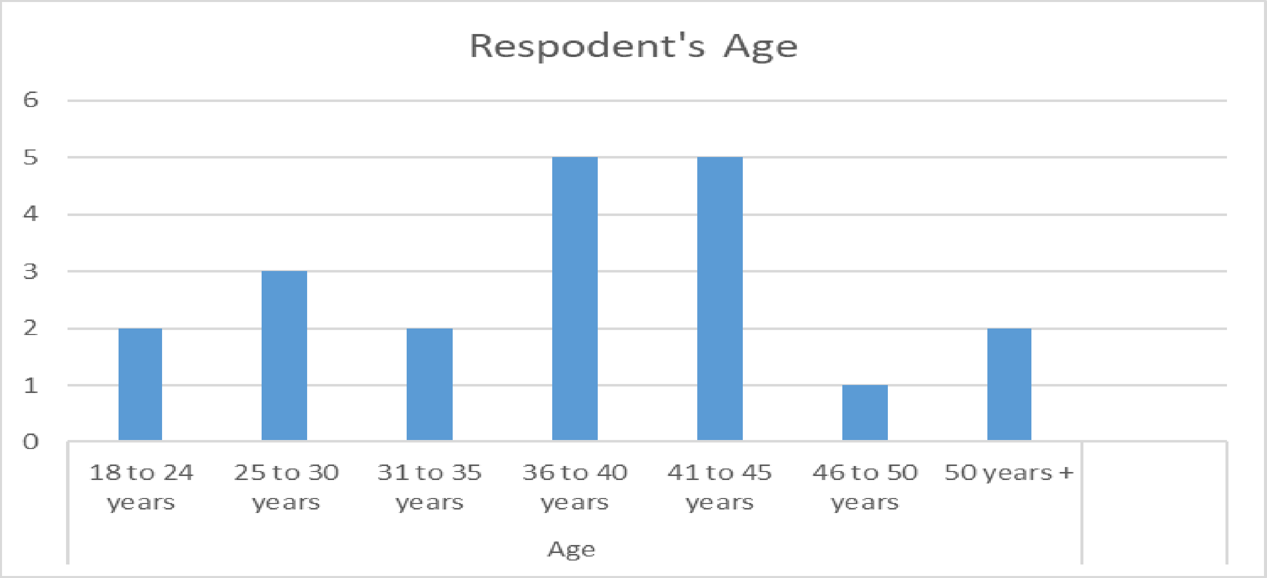

Fig 2 Respondent's age

The graph displays the age distribution of respondents. The most significant group is aged 36 to 40 years, with a count of 5 respondents. The 25 to 30 years and 41 to 45 years categories have 3 respondents each. The 18 to 24 years and 50 years+ categories have lower counts, with 1 and 2 respondents, respectively. Generally, the data indicates a concentration of respondents in the 36 to 40 age range.

4.2.3 Marital status of the respondents.

Table 1.2

Marital status of the respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Married	15	75.0	75.0	75.0
	Single	5	25.0	25.0	100.0
	Total	20	100.0	100.0	

The table 1.2 presents the marital status of respondents, showing that out of 20 valid responses, 15 respondents (75.0% of the total) are married, while 5 respondents (25.0% of the total) are single. The cumulative percent indicates that all respondents fall into these two categories, with 75.0% married and 100.0% when both categories are combined, highlighting a clear majority of respondents being married.

4.2.4 Career History

The table 1.3 provides insights into the distribution of respondents based on their experience duration, with a total of 20 valid responses.

Table 1.3

Respondent's Career history

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1- 3 years	4	20.0	20.0	20.0
	4-6 years	2	10.0	25.0	35.0
	7-9 years	3	15.0	25.0	45.0
	10 years and above	11	45.0	45.0	100.0
	Total	20	100.0	100.0	

Among the respondents, 4 respondents (20.0%) have 1-3 years of experience, 2 respondents (10.0%) fall into the 4-6 years category, bringing the cumulative percent to 30.0%. Additionally, 3 respondents (15.0%) have 7-9 years of experience, increasing the cumulative percent to 45.0%. Finally, 11 respondents (45.0%) have 10 years or more, leading to a cumulative total of 100.0%. This data indicates that the majority of respondents (55.0%) have 7 years or more of experience, with the largest group (45.0%) having 10 years or more, suggesting a well-experienced population.

4.2.5 Respondent's Qualification

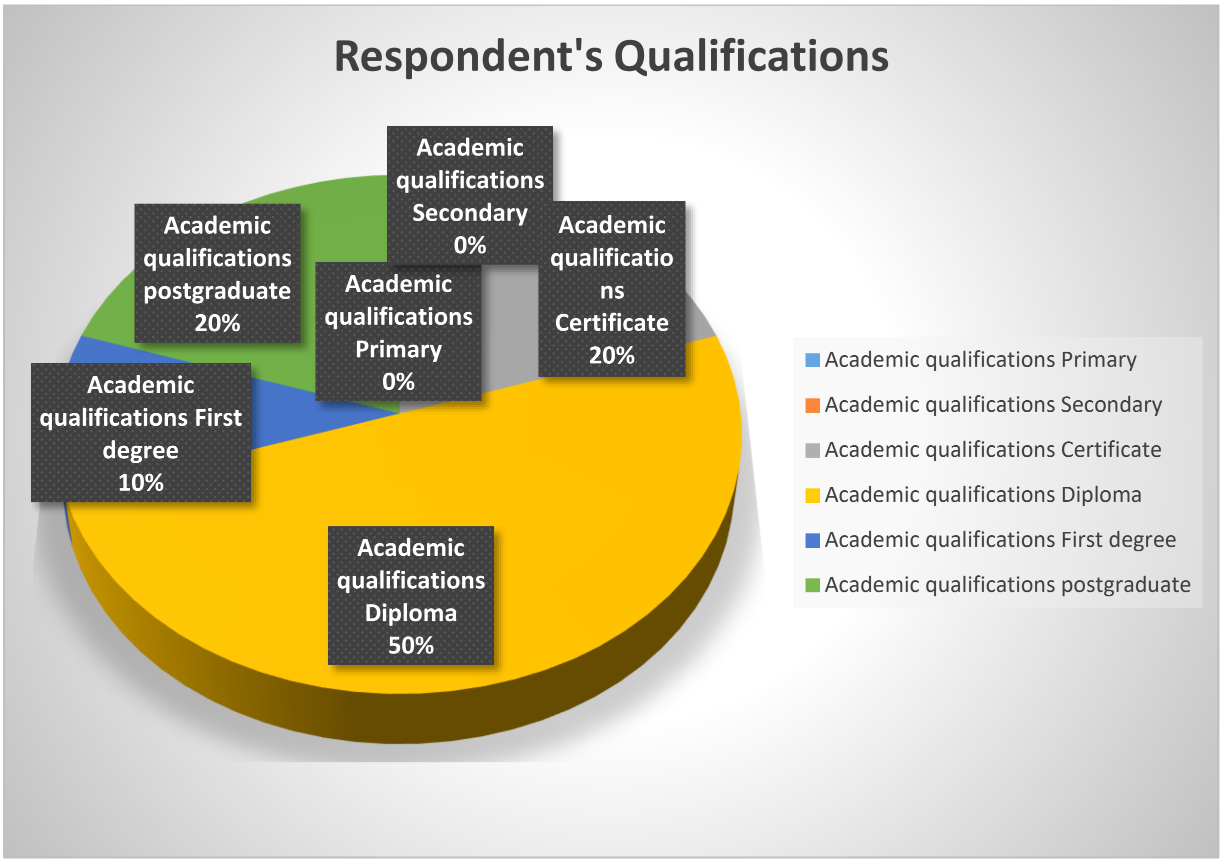

Fig 3 Respondent's qualification

The pie chart or *fig 3* illustrates the qualifications of respondents. The largest segment is for Diploma holders, comprising 50% of the total. Postgraduate qualifications account for 20%, while First degree and Secondary qualifications each represent smaller portions. Primary qualifications have no representation. This highlights that the majority of respondents possess diploma-level qualifications.

4.3 This section presents and analyzes the data about the main research objectives.

This section discusses the findings related to the study's main research objectives, which were to: To determine the challenges to reporting and prosecuting cybercrime in Bindura district.

To identify the barriers to reporting and prosecuting cybercrime in Bindura district.

To describe the nature of cybercrime that takes place in the Bindura district.

To recommend a cybercrime elimination guide to be used in the Bindura district

4.3.1 What are the biggest challenges to reporting and prosecuting cybercrime in Bindura district?

The chart or *Fig 4* outlines the major challenges to reporting and prosecuting cybercrime in Bindura district, revealing several key observations.

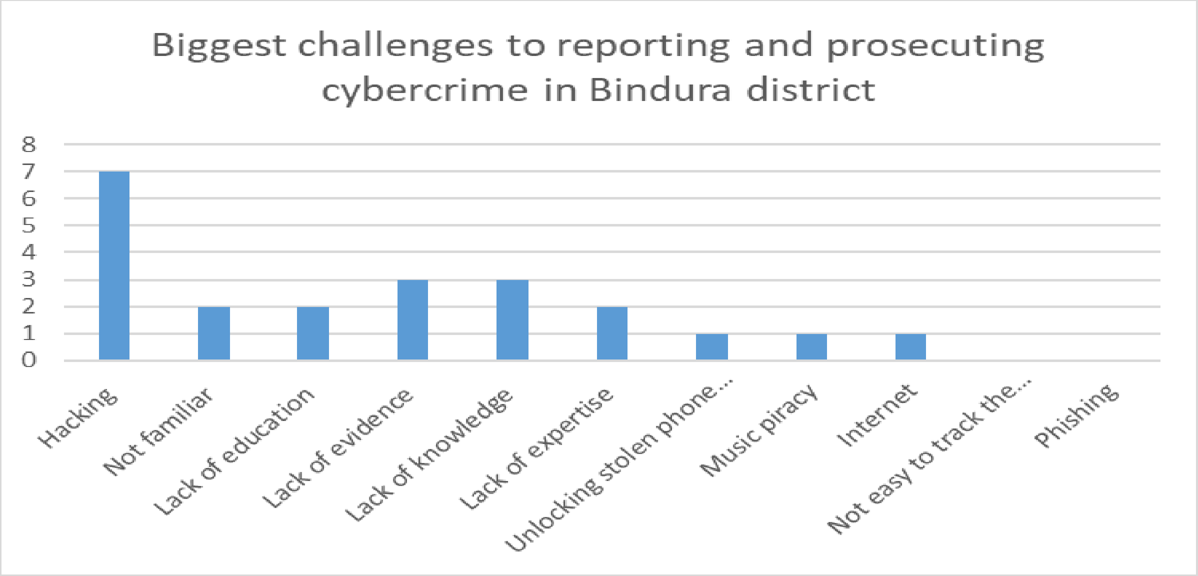

Fig 4 Challenges to reporting and prosecuting cybercrime

Hacking emerges as the most significant issue, indicating a high prevalence of incidents that complicate victims' efforts to report or seek prosecution. Additionally, a lack of familiarity and education about cybercrime contributes to a general unawareness that hampers effective reporting. Critical factors such as insufficient evidence and knowledge further complicate cases, as the absence of clear proof makes it difficult to build a solid case, while a lack of understanding prevents individuals from recognizing cybercrime. The challenge of unlocking stolen phones highlights the complexities involved in recovering such devices, potentially due to technological or legal barriers. Other issues, including music piracy, not easy to track the accurate cybercrime offender and phishing, are noted but are less significant than the primary challenges identified. This analysis sheds light on the challenges faced in Bindura regarding cybercrime and underscores critical areas for intervention.

4.3.2 What are the barriers to reporting and prosecuting cybercrime in Bindura district?

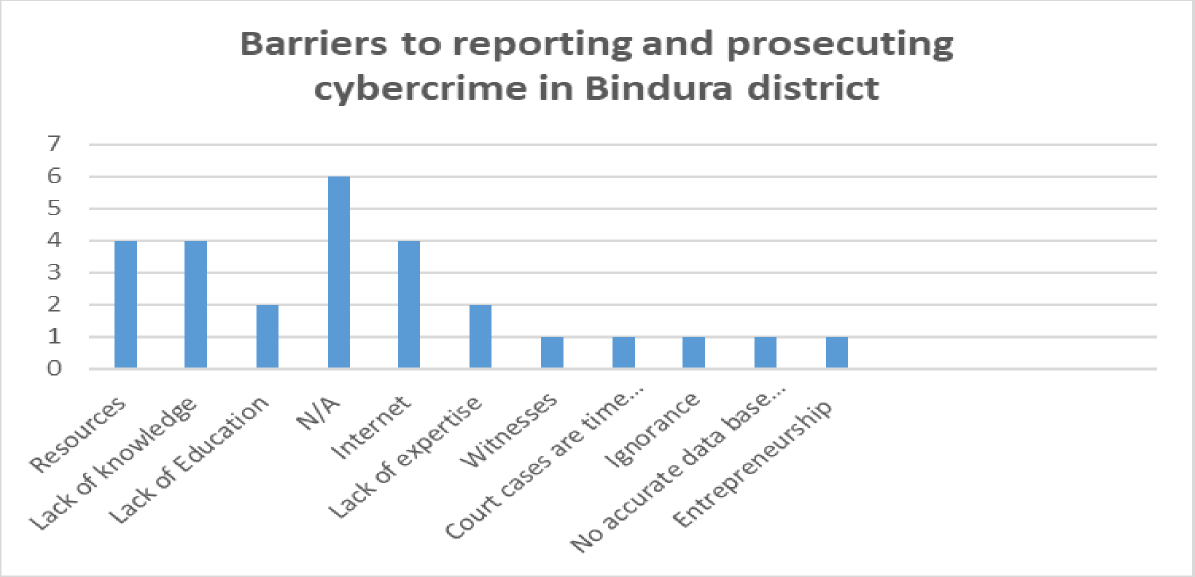

Fig 5 Barriers to reporting and prosecuting cybercrime

The chart or *fig 5* illustrates the barriers to reporting and prosecuting cybercrime in Bindura district, highlighting several significant factors that hinder effective action against these crimes. Among these barriers, the lack of resources stands out as a prominent issue. This suggests that both financial and technological support are insufficient for victims and law enforcement agencies, which can impede the investigation and prosecution of cybercrime.

Another critical barrier is insufficient knowledge and lack of education. These factors indicate that individuals may not fully understand cybercrime, its implications, or how to report it. This lack of awareness can lead to underreporting and ineffective prosecution. Additionally, the mention of the Internet as a barrier may imply connectivity problems or that the digital landscape itself poses challenges for reporting and prosecuting cybercrime.

The lack of expertise also presents a significant hurdle. It suggests that there may be insufficient trained professionals available to handle cybercrime cases effectively, which can affect both the investigation process and the prosecution of offenders. Furthermore, difficulties in finding witnesses and the challenges associated with court cases indicate that gathering testimony and navigating the legal system can be complicated, further complicating prosecution efforts.

Data management issues, such as "no accurate database" and "ignorance," reflect systemic problems in tracking and managing cybercrime data. These issues are essential for understanding crime trends and effectively prosecuting offenders. Lastly, the mention of entrepreneurship as a barrier suggests that potential victims in the business sector may lack the necessary knowledge or resources to protect themselves against cybercrime.

4.3.3 Does the cybercrime that takes place in Bindura district have social and economic effects on the residents and the community?

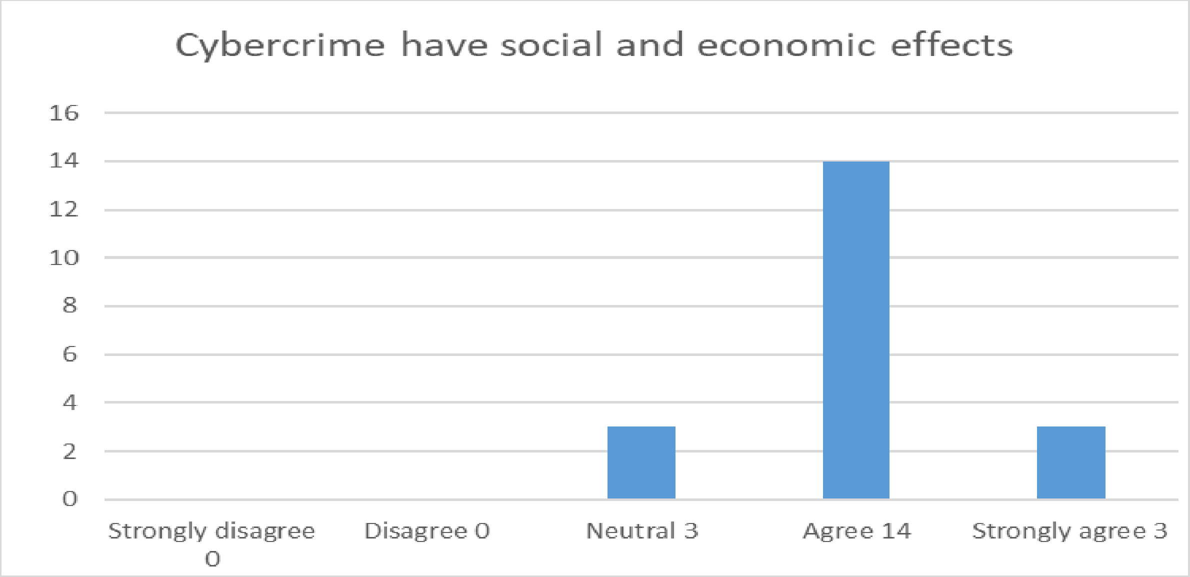

Fig 6 Social and Economic effects of cybercrime in Bindura district

The chart or *Fig 6* presents respondents' perceptions of the social and economic effects of cybercrime, indicating a significant consensus on its impact. A substantial majority, with 14 respondents, agree that cybercrime has notable social and economic effects, suggesting widespread recognition of the serious implications that these crimes can have on communities and economies. The responses labelled "Neutral" and "Disagree" are minimal, demonstrating that there is little contention regarding cybercrime's effects; most participants acknowledge its seriousness. Importantly, no respondents strongly disagreed with the statement, highlighting a unanimous recognition of the issue, even among those who may not feel strongly about its effects.

4.3.4 What cybercrime guide can be recommended to eliminate cybercrimes in Bindura District?

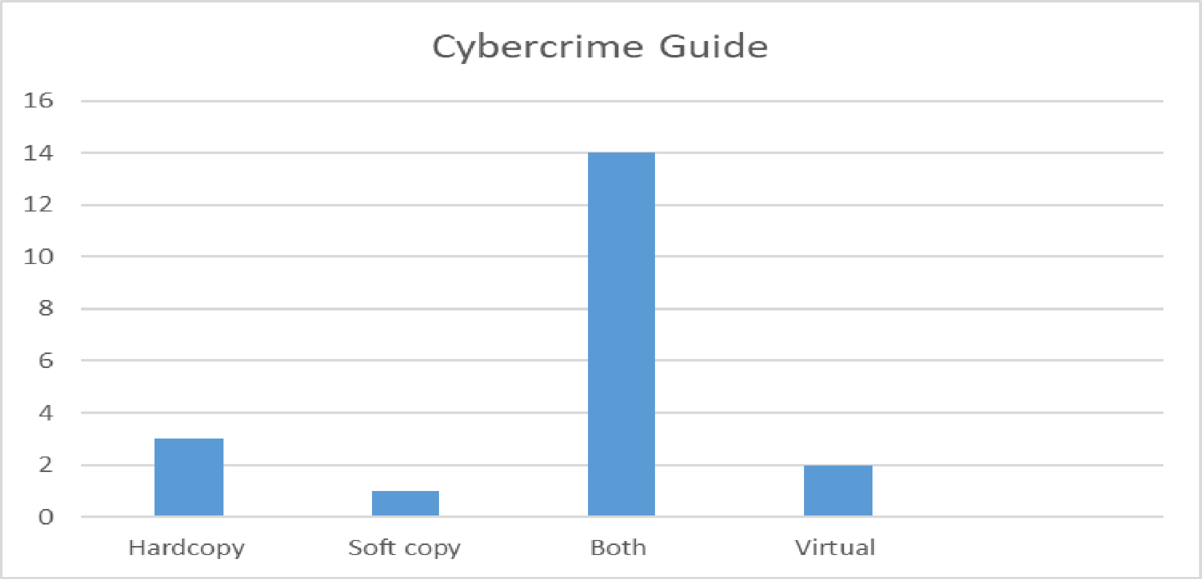

Fig 7 Cybercrime Guide to be to recommend

The chart or *Fig 7* illustrates preferences for formats of a cybercrime guide among respondents, revealing a clear inclination towards the option of "Both" hardcopy and soft copy formats, with 14 participants selecting this choice. This overwhelming preference indicates that individual's value having access to both physical and digital resources, suggesting a desire for flexibility in how they engage with the material. In contrast, the preference for hardcopy and virtual formats is notably low, with very few respondents opting for either.

4.4 Discussion

The study identified key challenges, including insufficient awareness, technological complexity, and jurisdictional issues. Routine Activity Theory (RAT) emphasises that the absence of capable guardians hinders law enforcement from countering cybercrime due to resource shortages (Amra, 2021). Many victims fail to report incidents due to fear or mistrust in law enforcement, aligning with Social Learning Theory (SLT), where victims perceive reporting as ineffective based on observed behaviors (Dearden & Parti, 2021). Technological limitations exacerbate the issue, as law enforcement lacks forensic tools, paralleling findings from Estonia's cybersecurity framework (von Solms, 2022). Additionally, cybercriminals exploit legal gaps, as seen in other African nations where outdated legislation creates prosecutorial challenges (Paul & Iyelolu, 2024). Strengthening cybersecurity laws and public education could mitigate these barriers.

Barriers also include low digital literacy, inadequate law enforcement training, and socio-cultural stigma. The study found that victims hesitate to report crimes due to limited awareness, mirroring findings on cybersecurity education gaps in Africa (Wilson, 2021). The Strain Theory suggests economic pressures influence cybercrime victimization, as financially constrained individuals lack access to protective technologies (Nickerson, 2023). Additionally, jurisdictional challenges hinder prosecution. Cybercriminals operating across borders complicate legal proceedings. This echoes findings from the Budapest Convention's limitations (Malunga, 2022). Weak institutional coordination further obstructs efficient case handling, akin to Nigeria's enforcement struggles (Arunga, 2023). Legal frameworks like Zimbabwe's Cyber and Data Protection Bill require enhancement to streamline investigations and establish specialized cybercrime units (Hilal et al., 2024).

The study highlights significant socio-economic consequences, including financial losses and reputational damage. Deterrence Theory emphasizes fear of punishment as a crime-prevention mechanism. However, Bindura's weak enforcement undermines deterrence. Cybercrime erodes community trust in digital transactions, hindering economic participation, as seen in Zimbabwean SMEs impacted by digital fraud (Ndawana & Chisambiro, 2024). Victims experience psychological distress and social stigma (Wilson, 2021). Financial institutions face security vulnerabilities due to inadequate cybersecurity infrastructure. This parallels Kenya's cyber challenges (Arunga, 2023). Community-driven awareness programs and improved cybersecurity policies can mitigate these effects.

The study found out that enhanced legal frameworks, community awareness, and law enforcement capacity building can help deal with cybrcrime. Routine Activity Theory suggests reducing crime opportunities by strengthening online surveillance and equipping law enforcement with digital forensic expertise (Amra, 2021). Educational initiatives on cyber hygiene, inspired by Estonia's cybersecurity model, could increase digital literacy and preventive actions (von Solms, 2022). Strengthening international collaborations through conventions like the Budapest Treaty would aid cross-border cybercrime prosecution (Malunga, 2022). Implementing AI-driven cybersecurity solutions, as utilized in Singapore, can bolster local defense against cyber threats (Alhalafi & Veeraraghavan, 2021). Community trust-building efforts, such as transparent reporting systems, can encourage victims to seek legal recourse, ensuring a safer digital environment for Bindura residents.

CHAPTER V

SUMMARY, CONCLUSIONS, RECOMMENDATIONS AND RECOMMENDATIONS FOR FURTHER STUDY

5.0 Introduction

This chapter focused on the summary, conclusions, and recommendations. The conclusions will address the four research questions outlined in Chapter 1. Recommendations to practice and further study are also be suggested in this chapter.

5.1 Summary

Hacking is the most pressing issue in Bindura, with a high incidence rate that complicates victims' ability to report or seek prosecution, exacerbated by a lack of education and awareness about cybercrime. Additionally, challenges such as insufficient evidence, difficulties in recovering stolen devices, and issues like music piracy and phishing further hinder effective reporting and intervention efforts.

The results highlights several barriers to reporting and prosecuting cybercrime in Bindura district, with a lack of resources, knowledge, and expertise being the most significant issues. Insufficient financial and technological support, coupled with a general lack of understanding about cybercrime and its implications, leads to underreporting and ineffective prosecution. Additionally, challenges such as connectivity issues, difficulties in gathering witness testimony, and systemic data management problems further complicate efforts to address cybercrime, particularly for potential victims in the business sector.

The results illustrates respondents' perceptions of the social and economic effects of cybercrime, showing a strong consensus on its significant impact. A majority of 14 respondents acknowledge the serious implications of cybercrime on communities and economies, with minimal neutral or disagreeing responses, indicating widespread agreement on the issue's seriousness and no strong dissent among participants.

The outcome shows that respondents overwhelmingly prefer a cybercrime guide in both hardcopy and soft copy formats, with 14 participants choosing this option, indicating a desire for flexibility in accessing resources. In contrast, preferences for exclusively hardcopy or digital formats are minimal, highlighting a clear inclination towards having both options available.

5.2 Conclusions

Hacking poses a critical challenge in Bindura. It significantly hinders victims' ability to report incidents and seek justice. This is exacerbated by a lack of education and awareness about cybercrime. This situation highlights the urgent need for targeted educational initiatives and resources to empower individuals and facilitate effective reporting.

The barriers to reporting and prosecuting cybercrime in Bindura are largely attributed to insufficient resources, knowledge, and expertise. Addressing these challenges is vital for enhancing the community's capacity to respond to cybercrime effectively, particularly for vulnerable sectors such as businesses.

The strong consensus among respondents regarding the social and economic effects of cybercrime underscores its serious implications for communities and economies. This widespread recognition calls for ongoing efforts to raise awareness and implement strategies that mitigate the impacts of cybercrime.

The preference for a cybercrime guide in both hardcopy and soft copy formats indicates a clear demand for flexible access to information. Providing resources in multiple formats is essential to cater to diverse user needs and enhance the overall effectiveness of educational materials on cybercrime.

5.3 Recommendations

In light of the findings, it is essential to organize community workshops that educate citizens about cybercrime and develop user-friendly reporting mechanisms to assist victims in documenting their experiences. Strengthening collaboration between communities and law enforcement will create an environment where victims feel safe and supported when coming forward. Establishing support systems for victims can help them navigate the complexities of evidence collection and unfamiliarity with the legal process. Additionally, enhancing the legal framework surrounding cybercrime will improve prosecution efforts and provide clearer pathways for victim support.

The community's strong awareness of cybercrime presents an opportunity to advocate for more effective measures against it. Stakeholders, including local governments, law enforcement, and community organizations, should prioritize education, resource allocation, and policy development to address this pressing issue. Programs aimed at raising awareness socioeconomic impacts of cybercrime can further engage the community and foster a collective response to prevention and reporting.

Moreover, it is crucial to encourage policymakers to devise strategies that mitigate the effects of cybercrime, thereby enhancing community resilience. Engaging the public in discussions about cybercrime will promote the sharing of best practices and foster a collaborative approach to tackling the problem. This highlights the urgent need for measures to address the significant ramifications of cybercrime on society.

To effectively combat cybercrime, there should be training programs to enhance knowledge and skills among both law enforcement and community members. Increasing resources, including funding and technology, is vital for successful prosecution. Additionally, creating accurate databases and improving data management systems will facilitate tracking cybercrime and understanding its broader impact.

Implementing community education initiatives will empower individuals to recognize and report cybercrime, while strengthening the legal framework will provide clearer avenues for prosecution and victim support. Engaging cybersecurity experts to train law enforcement can further improve the handling of cybercrime cases in the Bindura district.

Finally, a thorough exploration of cybercrime awareness among various demographics, such as students, business owners, and law enforcement personnel, is recommended to identify knowledge gaps and misconceptions that may contribute to vulnerability and underreporting. This investigation should be complemented by an assessment of law enforcement capabilities in digital forensics and cyber law. Understanding the economic impact of cybercrime on small and medium enterprises (SMEs) in Bindura will also provide valuable insights into specific threats and coping strategies. By evaluating digital literacy and cyber hygiene practices, targeted educational initiatives can be developed to enhance community resilience against cyber threats.

5.4 Recommendations for Further Study

It is recommended to conduct a study to assess the effectiveness of existing community awareness programs on cybercrime in Bindura District. This research can explore how these programs influence reporting behaviours and the perceived effectiveness of law enforcement responses.

It is also recommended analyse the specific economic implications of cybercrime on small and medium enterprises (SMEs) in Bindura. This study could focus on identifying vulnerabilities, coping strategies, and the overall impact on business operations and community resilience against cyber threats.

References

Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology, 7(1), 138-158.

Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. Wireless Personal Communications, 119, 2603-2637.

Adhabi, E & Anozie, B (2017). Literature review for the type of interview in qualitative research, *international journal of education*, ISSN 1948-5476.vol 9 No3 URL:https://doi.org/10.5296/ije.v9i3.11483.

Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.

Aghayeva, S. (2023, May). Technical means of information security. In 1st INTERNATIONAL CONFERENCE ON THE 4th INDUSTRIAL REVOLUTION AND INFORMATION TECHNOLOGY (Vol. 1, No. 1, pp. 296-299). Azərbaycan Dövlət Neft və Sənaye Universiteti.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939-953.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future internet, 12(10), 168.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & security, 99, 102030.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. Heliyon, 10(12).

Alhalafi, N., & Veeraraghavan, P. (2021). Cybersecurity policy framework in Saudi Arabia: Literature review. Frontiers in Computer Science, 3, 736874.

Alhamdani, F (2016). An introduction to qualitative research data analysis artistic approach, *international journal of development research* vol.06, issue, 12pp.10616

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. International Journal of Educational Reform, 33(1), 101-121.

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

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International Journal of Law and Policy, 2(5), 28-36.

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. Journal of Infrastructure, Policy and Development, 8(10), 6007.

Allibang, S. (2020). Research methods: Simple, short, and straightforward way of learning methods of research. Sherwyn Allibang.

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal: A Global Perspective, 30(4), 189-204.

Alshengeeti, H (2014). Interviewing as a data collection method: a critical review, URL:https://dx.doi.org/10.5430/erv5nlp39

Alyahyan, E., & Düştegör, D. (2020). Predicting academic success in higher education: literature review and best practices. International Journal of Educational Technology in Higher Education, 17(1), 3.

Arunga, B. H. (2023). Countering Cybercrime in Kenya: Our Shared Responsibility (Doctoral dissertation, University of Nairobi).

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Bajpai, P., & Enbody, R. (2020, June). An empirical study of key generation in cryptographic ransomware. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.

Balantrapu, S. S. (2024). AI for Predictive Cyber Threat Intelligence. International Journal of Management Education for Sustainable Development, 7(7), 1-28.

Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. South African Journal of Business Management, 51(1), 1-10.

Bates, L., & Anderson, L. (2021). Young drivers, deterrence theory, and punishment avoidance: a qualitative exploration. Policing: A Journal of Policy and Practice, 15(2), 784-797.

Bellin, J. (2020). Theories of Prosecution. California Law Review, 108(4), 1203-1253.

Billah, M. (2021). Prosecuting crimes against humanity and genocide at the international crimes tribunal Bangladesh: An approach to international criminal Law standards. Laws, 10(4), 82.

Biwer, F., oude Egbrink, M. G., Aalten, P., & de Bruin, A. B. (2020). Fostering effective learning strategies in higher education–a mixed-methods study. Journal of Applied Research in Memory and Cognition, 9(2), 186-203.

Browning, C. R., Pinchak, N. P., & Calder, C. A. (2021). Human mobility and crime: Theoretical approaches and novel data collection strategies. Annual Review of Criminology, 4(1), 99-123.

Bun, M. J., Kelaher, R., Sarafidis, V., & Weatherburn, D. (2020). Crime, deterrence and punishment revisited. Empirical economics, 59(5), 2303-2333.

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

Chan-Tin, E., & Stalans, L. J. (2023). Phishing for profit. In Handbook on Crime and Technology (pp. 54-71). Edward Elgar Publishing.

Chawki, M. (2022, March). Cybercrime and the Regulation of Cryptocurrencies. In Future of Information and Communication Conference (pp. 694-713). Cham: Springer International Publishing.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10(1), 1-10.

Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. Review of International Geographical Education Online, 11(7).

Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity. Engineering International, 10(2), 69-84.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society, 32(1), 103-124.

Cook, L. D., Thompson, C., Weaver, S., & Weaver, L. (2020). Mixed methods research: Exploring its complexities and challenges. Caribbean Journal of Mixed Methods Research, 1(1), 167-190.

Cresswell, J (2014). *Research design: qualitative, quantitative and mixed approaches*, 4th Ed, SAGE: London

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. Trends and Issues in Crime and Criminal Justice [electronic resource], (635), 1-20.

Crowe, S, Cresswell, Robertson, A, (2011). The case study approach, BMC Med Res Methodology 11,100(2011).https://doi.org/10-1186/1471-2288-11-100

Cunha, M& Moreira, F (2011). *Handbook of research on mobility and computing: evolving technologies and ubiquitous impacts*, volume 2, IGL global: Portugal

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. Journal of Practical Studies in Education, 2(2), 25-36.

De Costa, P. I., Randez, R. A., Her, L., & Green-Eneix, C. A. (2021). Navigating ethical challenges in second language narrative inquiry research. System, 102, 102599.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., ... & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. Policing: A Journal of Policy and Practice, 15(2), 1429-1445.

Dearden, T. E., & Gottschalk, P. (2024). Convenience theory and cybercrime opportunity: An analysis of online cyber offending. Deviant Behavior, 45(3), 348-360.

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. American Journal of Criminal Justice, 46(6), 935-955.

Denzin, N, K & Lincoln, Y,S, (2011). *Introduction: The discipline and practice of qualitative research: the handbook of quantitative research,* 4th Ed, sage.

Didenko, A. N. (2020). Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review, 25(1), 125-167.

DiGaetano, R (2012). Sample frame and related sample design issues for surveys of physician practices, volume: 36 issue 3, pages 296-329, *journal of Pub Med* http://doi.org/10.1177/0163278713496566

Drabent, K., Janowski, R., & Mongay Batalla, J. (2024). How to Circumvent and Beat the Ransomware in Android Operating System—A Case Study of Locker. CB! tr. Electronics, 13(11), 2212.

Dunlea, R. R. (2022). "No idea whether he's Black, White, or purple": Colorblindness and cultural scripting in prosecution. Criminology, 60(2), 237-262.

Dunne, C., & Ustundag, B. G. (2020, January). Successfully managing the literature review and write-up process when using grounded theory methodology—A dialogue in exploration. In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research (Vol. 21, No. 1).

Ene, W. R., & Imo, A. S. (2024). Cybercrime and its implications for human capital development: A study of Otuoke Community, Fuo Students. Fuoye Journal of Criminology and Security Studies, 3(2).

Fabbrini, F., & Celeste, E. (2020). The right to be forgotten in the digital age: The challenges of data protection beyond borders. German law journal, 21(S1), 55-65.

Fan, D., Breslin, D., Callahan, J. L., & Iszatt-White, M. (2022). Advancing literature review methodology through rigour, generativity, scope and transparency. International Journal of Management Reviews, 24(2), 171-180.

Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M., & Bilan, O. (2021, September). Ransomware attacks: risks, protection and prevention measures. In 2021 11th international conference on advanced computer information technologies (ACIT) (pp. 473-478). IEEE.

Farquhar, J (2012), *Case study research for business*, SAGE: London

Fink, A, (2014), *conducting research literature reviews from the internet to paper,* 4th Ed, SAGE: Los Angeles

FoodRisc Resource Centre (2016). https://resource centre.foodrisc.org/mixed-methods-research-185.

Goni, O. (2022). Cybercrime and its classification. Int. J. of Electronics Engineering and Applications, 10(1), 17.

Goni, O., Ali, M. H., Showrov, M. M. A., & Shameem, M. A. (2022). The basic concept of cybercrime. Journal of Technology Innovations and Energy, 1(2), 16-24.

Goundar, S (2013). Research methodology and research method http://www.researchgate.net/publication/333015026-chapter 3-research-methodology and research-methods/stats

Govender, I., Watson, B. W. W., & Amra, J. (2021, February). Global virus lockdown and cybercrime rate trends: A routine activity approach. In Journal of Physics: Conference Series (Vol. 1828, No. 1, p. 012107). IOP Publishing.

Guetterman, T. C., Fàbregues, S., & Sakakibara, R. (2021). Visuals in joint displays to represent integration in mixed methods research: A methodological review. Methods in Psychology, 5, 100080.

Harding, T & Whiteheard, D, (2018). Analysing data in qualitative research https://www.researchgate.net/publication/255950505

Hendren, K., Newcomer, K., Pandey, S. K., Smith, M., & Sumner, N. (2023). How qualitative research methods can be leveraged to strengthen mixed methods research in public policy and public administration? Public Administration Review, 83(3), 468-485.

Hossain, R. (2022). Ethical Hacking Using Penetration Testing (Doctoral dissertation, East West University).

Igwenagu, C (2016). Fundamentals of research methodology and collection, edition-current, Lambert academic publishing

Isakov, A., Urozov, F., Abduzhapporov, S., & Isokova, M. (2024). Enhancing Cybersecurity: Protecting Data In The Digital Age. Innovations in Science and Technologies, 1(1), 40-49.

Islamia, J (2016). Research design https://www.researchget.net/publications/308915548

Jackson, S (2012). *Research methods and statistics: a critical thinking approach*, 4th Ed, Wadsworth publishers

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. The Journal of Criminal Law, 84(5), 427-450.

Karunarathna, I., Gunasena, P., Hapuarachchi, T., & Gunathilake, S. (2024). Comprehensive data collection: Methods, challenges, and the importance of accuracy.

Kehinde Oyedeji, J., & Olamide Badmos, H. (2022). Social construction of internet fraud as innovation among youths in Nigeria. International Journal of Cybersecurity Intelligence & Cybercrime, 5(1), 23-42.

Khater, M., Ibrahim, O., Sayed, M. N. E., & Faik, M. (2024). Legal frameworks for sustainable tourism: balancing environmental conservation and economic development. Current Issues in Tourism, 1-22.

Knott, E., Rao, A. H., Summers, K., & Teeger, C. (2022). Interviews in the social sciences. Nature Reviews Methods Primers, 2(1), 73.

Koegl, C. J., & Farrington, D. P. (2022). Advancing knowledge about motivations for criminal offending. Victims & Offenders, 17(3), 313-334.

Kumar, S. (2023). CYBER CRIME: A Review. International Journal of Advanced Scientific Innovation, 5(12).

Lim, W. M. (2024). What is qualitative research? An overview and guidelines. Australasian Marketing Journal, 14413582241264619.

Maingi, E. M. (2022). A System for reporting online child abuse and offenders (Doctoral dissertation, Strathmore University).

Maluleke, W. (2023). Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. International Journal of Social Science Research and Review, 6(6), 223-243.

Malunga, S. (2022). A history of atrocity: Patterns, perpetrators and prospects for accountability for international crimes in Zimbabwe. In National accountability for international crimes in Africa (pp. 527-582). Cham: Springer International Publishing.

Martin, E. V. (2022). The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training (Doctoral dissertation, Walden University).

McKoy, C. (2021). Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level (Doctoral dissertation, Walden University).

McKoy, C. (2021). Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level (Doctoral dissertation, Walden University).

Miró-Llinares, F., & Moneva, A. (2020). Environmental criminology and cybercrime: Shifting focus from the wine to the bottles. In The Palgrave handbook of international cybercrime and cyberdeviance (pp. 491-511). Cham: Springer International Publishing.

Monaghan, R. M. (2020). Cybercrime response capabilities and capacity: an evaluation of local law enforcement's response to a complex problem (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

Morrison-Smith, S., & Ruiz, J. (2020). Challenges and barriers in virtual teams: a literature review. SN Applied Sciences, 2(6), 1-33.

Nazaretian, Z., & Fitch, C. (2021). Comparing the lifestyles of victims: A routine activity theory assessment of repeat victimization in Canada. Journal of Community Safety and Well-Being, 6(2), 56-65.

Nickerson, C. (2023). Merton's strain theory of deviance and anomie in sociology.

Nosál, J. (2023). Crime in the Digital Age: A New Frontier. In The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network (pp. 177-193). Cham: Springer International Publishing.

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Computers in human behavior, 120, 106745.

Panorios, M. (2024). Phishing attacks detection and prevention (Master's thesis, Πανεπιστήμιο Πειραιώς).

Paul, P. O., & Iyelolu, T. V. (2024). Anti-Money laundering compliance and financial inclusion: A technical analysis of Sub-Saharan Africa. *GSC Advanced Research and Reviews*, 19(3), 336-343

Payne, B., & Mienie, E. (2021, June). Multiple-extortion ransomware: The case for active cyber threat intelligence. In ECCWS 2021 20th European Conference on Cyber Warfare and Security (Vol. 6, pp. 331-336). Academic Conferences Inter Ltd.

Perez-Vincent, S. M., Abril, V., Chen, C., Tayo, T., & Jimenez, A. U. (2024). Crime Underreporting in Latin America and the Caribbean.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

Petal, M., Ronan, K., Ovington, G., & Tofa, M. (2020). Child-centred risk reduction and school safety: An evidence-based practice framework and roadmap. International journal of disaster risk reduction, 49, 101633.

Piacquadio, J. (2024). DEVELOPMENT OF A FRAMEWORK TO EXPLAIN AND JUSTIFY CYBERSECURITY INVESTMENT:-AN ACTION RESEARCH INQUIRY (Doctoral dissertation, University of Liverpool).

Piquero, N. L., Piquero, A. R., Gies, S., Green, B., Bobnis, A., & Velasquez, E. (2022). Preventing identity theft: perspectives on technological solutions from industry insiders. In The New Technology of Financial Crime (pp. 163-182). Routledge.

Powers, R. A., Cochran, J. K., Maskaly, J., & Sellers, C. S. (2020). Social learning theory, gender, and intimate partner violent victimization: A structural equations approach. Journal of interpersonal violence, 35(17-18), 3554-3580.

Rahman, M. M. (2023). Sample size determination for survey research and non-probability sampling techniques: A review and set of recommendations. *Journal of Entrepreneurship, Business and Economics, 11*(1), 42-62.

Rapisarda, S. S., & Kras, K. R. (2023). Cyberstalking. Handbook on Crime and Technology, 303-333.

Raul, A. C. (Ed.). (2021). The privacy, data protection and cybersecurity law review. Law Business Research Limited.

Raza, S. A., Shaikh, M., & Tahira, K. (2023). Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances. Inf. Dyn. Appl, 2(3), 126-134.

Rumjaun, A., & Narod, F. (2020). Social learning theory—albert bandura. Science education in theory and practice: An introductory guide to learning theory, 85-99.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 100034.

Schunk, D. H., & DiBenedetto, M. K. (2022). Academic self-efficacy. In Handbook of positive psychology in schools (pp. 268-282). Routledge.

Sharma, S. (2024, February). Digital Forensics: Legal Standards and Practices in Cybercrime Investigation. In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) (pp. 1-6). IEEE.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756.

Shravasti, S. S., & Chavan, M. (2021). Smishing detection: Using artificial intelligence. Int. J. Res. Appl. Sci. Eng. Technol, 9(8), 2218-2224.

Silic, M., & Lowry, P. B. (2021). Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes. Information Systems Frontiers, 23, 329-341.

Smith, T. (2021). A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime.

Sukmawati, S. (2023). Development of quality instruments and data collection techniques. Jurnal Pendidikan Dan Pengajaran Guru Sekolah Dasar (JPPGuseda), 6(1), 119-124.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748-1774.

Suzuki, Y. E., & Monroy, S. A. S. (2022). Prevention and mitigation measures against phishing emails: a sequential schema model. Security Journal, 35(4), 1162-1182.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series, 33, 2020-01.

Taherdoost, H. (2021). Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. International Journal of Academic Research in Management (IJARM), 10(1), 10-38.

Taruvinga, F. (2020). Emerging Cyber Security Threats: A Comparative Study of Kenya and Zimbabwe (Doctoral dissertation, University of Nairobi).

Tatara, B. A., Abdurachman, B., Mustofa, D. L., & Yacobus, D. (2023). The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation. NUANSA: Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam, 20(1), 19-37.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education (JASE), 4(1), 1-20.

Tzagkarakis, S. I., & Kritas, D. (2023). Mixed research methods in political science and governance: approaches and applications. Quality & quantity, 57(Suppl 1), 39-53.

Uzoka, N. C. (2020). Cyber Security and Latest Development: Towards Effective Global Regulation and Governance in Cyberspace. IRLJ, 2, 55.

Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age. John Wiley & Sons.

Wang, S. Y. K., Hsieh, M. L., Chang, C. K. M., Jiang, P. S., & Collaboration between law enforcement agencies in combating cybercrime: implications of a taiwanese case study about ATM hacking. International journal of offender therapy and comparative criminology, 65(4), 390-408.

Whelan, C., & Harkin, D. (2021). Civilianising specialist units: Reflections on the policing of cyber-crime. Criminology & criminal justice, 21(4), 529-546.

Wright, D. C. S. (2023). Geographical Aspects of Cybercrime: A Literature Review. Available at SSRN 4521486.

Xu, T., Singh, K., & Rajivan, P. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics, 108, 103908.

APPENDICES

Questionnaire

QUESTIONNAIRE

Introduction

My name is Makosa John (B222403A**)** a student at the Bindura University doing Honors Degree in intelligence and security studies. I am carrying out a research study on the topic ***"Challenges and barriers to reporting and prosecuting cybercrime in Bindura district".*** You have been randomly selected to take part in this study. Could you please assist by completing this questionnaire? Participation in this survey is voluntary. No question is compulsory. There are no right or wrong answers. We just want your opinion. All your responses are strictly confidential and will only be used for this study. The responses you will give will be organised in such a way that neither your name nor your organisation will be identified.

Instructions:

a) Please read and understand the information in all sections carefully.

b) Kindly be as honest as possible when giving your responses.

c) For further enquires please do not hesitate to consult me.

d) Please tick in the correct box.

e) Do not write your name on this questionnaire.

1. Gender

- Male
- Female

2. Age

- 18 to 24 years
- 25 to 30 years

- 31 to 35 years
- 36 to 40 years
- 41 to 45 years
- 46 to 50 years
- 50 years and above

3. Marital status

- married
- single
- Separated
- divorced
- widow

4. Academic qualifications

- Primary
- secondary
- Certificate
- Diploma
- First Degree
- Postgraduate

5. Years of work experience

Less than 1 year	1-3years	4-6 years	7 -9 years	10 years +

6. Participant's experience

a. **In** general, how do you describe your experience at present?

- Very poor
- Poor
- Not Sure
- Good
- excellent

7. Instructions: Please tick where applicable

a. Have you ever faced challenges to reporting cybercrime in Bindura district?

- Never faced any challenges
- Rarely faced challenges
- Occasionally faced challenges
- Frequently faced challenges

- Always faced challenges

b. Have you ever faced challenges to prosecuting cybercrime in Bindura district?

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

c. Do you believe that there are barriers to reporting cybercrime in Bindura district?

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

d. Do you believe that there are barriers to prosecuting cybercrime in Bindura district?

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

e. If you answered yes to parts (a) and (b), give examples of challenges and barriers you have faced to reporting and prosecuting cybercrime.

  i. Give examples of the challenges you have faced.

____

____

____

___

____

ii. Give examples of the barriers

f. Do you think the cybercrime that takes place in Bindura district have social and economic effects on the residents and the community?

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

g. What cybercrime guide can be developed to eliminate cybercrimes in Bindura District?

Hardcopy	Softcopy	Both	Virtual

h. What are the major cybercrime activities in Bindura district?

phishing	identity theft	hacking	distributing child pornography	Malware attacks	Other (Specify)

g. Have you ever experienced mild or fatal side effects from cybercrime?

- Never experienced any side effects
- Rarely experienced mild side effects
- Occasionally experienced moderate side effects
- Frequently experienced severe side effects
- Always experienced fatal side effects

h. What do you prefer local cybercrime guide based on local information?

Local Cybercrime Guide	Non-local Cybercrime Guide

8. Indicate the extent to which you agree with the following statements by ticking in the appropriate box

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Bindura residents are following a local cybercrime guide (LCG)					
Bindura residents are following a nonlocal cybercrime guide (nLCG)					
Bindura district has the biggest challenges to reporting and prosecuting cybercrime					
The anti-cybercrime programs currently being used in Bindura have impacted positively on socially and economically					
The barriers to reporting and prosecuting cybercrime in Bindura district have been eliminated					
The law enforcement agents have put in place cybercrime guide to eliminate cybercrimes in Bindura District.					
Local resident receives regular anti-cybercrime awareness campaigns					

The Bindura district is local cybercrime guide to combat cybercrime.					
The law enforcement agents are closely monitoring and track down every cybercrime attack on the local residents					

Interview guide

Bindura University
of Science Education

INTERVIEW GUIDE

Introduction

My name is Makosa John (B222403A**)** a student at the Bindura University doing Honors Degree in intelligence and security studies. I am conducting a research study on the topic ***"Challenges and barriers to reporting and prosecuting cybercrime in Bindura district".*** You have been randomly selected to take part in this study. Could you please assist by completing this interview guide? Participation in this survey is voluntary. No question is compulsory. There are no right or wrong answers. We want your opinion. All your responses are strictly confidential and will only be used for this study. The responses you will give will be organised in such a way that neither your name nor your organisation will be identified.

Demographic Questions:

1. Gender

- Male
- Female

2. Age

- 18 to 24 years
- 25 to 30 years

- 31 to 35 years
- 36 to 40 years
- 41 to 45 years
- 46 to 50 years

3. Marital status

- married
- single
- Separated
- divorced
- widow

4. Academic qualifications

- Primary
- secondary
- Certificate
- Diploma
- First Degree
- Postgraduate

5. Years of work experience

Less than 1 year	1-3years	4-6 years	7 -9 years	10 years +

Interview Questions

6. Have you ever faced challenges to reporting cybercrime in Bindura district?

7. Have you ever faced challenges to prosecuting cybercrime in Bindura district?

8. Do you believe that there are barriers to reporting cybercrime in Bindura district?

9. Do you believe that there are barriers to prosecuting cybercrime in Bindura district?

10. Do you think the cybercrime that takes place in Bindura district have social and economic effects on the residents and the community?

11. What cybercrime guide can be developed to eliminate cybercrimes in Bindura District?

12. What are the major cybercrime activities in Bindura district?

13. Have you ever experienced mild or fatal side effects from cybercrime?

14. What do you prefer local cybercrime guide based on local information?

THANK YOU